Dell Data Guardian

Guia do administrador para Windows, Mac, dispositivos móveis e Web v2.0

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

AVISO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

Guia do administrador para Windows, Mac, dispositivos móveis e Web

2018 - 08

Rev. A01

Índice

1 Introdução 5
Before You Begin 5
Entre em contato com o Dell ProSupport 5

2 Requisitos 6
Dell Server 6
Data Guardian para Windows 6
Pré-requisitos 7
Hardware 7
Sistemas operacionais 7
Provedores de armazenamento em nuvem 8
Microsoft Office 8
Data Guardian para Mac 9
Sistemas operacionais 9
Provedores de armazenamento em nuvem 9
Aplicativo móvel para o Data Guardian 10
Data Guardian para Web 10
Navegadores da Web 11
Suporte a idiomas 11

3 Configurar e instalar o Data Guardian no Windows 12
Configurações do registro do cliente do Data Guardian 12
Configurar o servidor para o Data Guardian 12
Configurar o Dell Security Management Server Virtual para Data Guardian 13
Configurar o Dell Security Management Server para Data Guardian 13
Desativar o EMET ou Exploit Guard da Microsoft para aplicativos gerenciados 15
Gerenciar perfis de provedor de proteção de armazenamento 15
Permitir/negar usuários da lista de acesso completo/lista negra 16
Instalar o Data Guardian 16
Pastas existentes com arquivos não-criptografados 17
Menu de Gerenciar pastas 17
Instalar o Data Guardian interativamente no Windows 17
Instalar o Data Guardian com a linha de comando 18
Set GPO on Domain Controller to Enable Entitlements 19
Desinstalar o Data Guardian 20
Usar o Data Guardian com o Dropbox for Business 20
Política para contas da empresa e pessoais 20
Pastas empresariais e pessoais 21
Exibir relatórios 21
Solução de problemas do Data Guardian 22
Usar a tela Detalhes 22
Usar a tela Detalhes aprimorados 22
Mostrar arquivos de log 22

Solução de problemas de ativação automática..... 22
Fornecer direitos de gerenciamento temporário de pastas..... 22
Frequently Asked Questions..... 23

4 Configurar e instalar o Data Guardian no Mac..... 26
Tarefas do servidor..... 26
Pré-requisitos..... 26
Políticas..... 26
Configurar o Security Server para permitir downloads de cliente de nuvem..... 27
Permitir/negar usuários da lista de acesso completo/lista negra..... 28
Tarefas de cliente..... 29
Pré-requisitos..... 29
Práticas recomendadas..... 29
Instalar o cliente..... 29
Ativação do usuário final..... 31
Desinstalar o Data Guardian..... 31

5 Configurar e instalar o Data Guardian para o cliente Web..... 32
Fazer download do arquivo OVA..... 32
Instalar o Data Guardian para Web..... 32
Abrir o Management Console..... 34
Tarefas básicas de configuração do terminal do Data Guardian..... 34
Alterar Nome de host..... 34
Alterar configurações de rede..... 35
Alterar senhas de usuário..... 35
Habilitar o SSH..... 36
Iniciar ou parar serviços..... 36
Reinicializar o dispositivo..... 36
Desligar o dispositivo..... 36
Tarefas do administrador..... 36
Definir ou alterar o idioma do terminal..... 36
Gerar um log de instantâneos do sistema..... 37

1

Introdução

Todas as informações sobre as políticas e suas descrições podem ser encontradas no AdminHelp.

Before You Begin

1 Instale o Dell Server antes de implementar os clientes. Localize o guia correto conforme mostrado abaixo, siga as instruções descritas e retorne para este guia.

- *Security Management Server Installation and Migration Guide*
- *Security Management Server Virtual Quick Start Guide and Installation Guide*
- Verifique se as políticas estão definidas conforme desejado. Procure através do AdminHelp, disponível a partir do **?** no canto superior direito da tela. O AdminHelp é uma ajuda no nível de página desenvolvida para ajudar você a definir e modificar políticas e compreender as suas opções com o Dell Server.

2 Leia completamente o capítulo Requisitos deste documento.

3 Implemente os clientes para os usuários.

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, veja Números de telefone internacionais do Dell ProSupport.

2

Requisitos

Dell Server

O Data Guardian para Windows, Mac e móvel exige o Security Management Server ou o Security Management Server Virtual v9.6 ou superior. O cliente Web do Data Guardian exige o Security Management Server ou o Security Management Server Virtual v9.8 ou superior. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Security Management Server Virtual).

Data Guardian para Windows

- As práticas recomendadas de TI devem ser seguidas durante a implementação. Isso inclui, sem limitações, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários.
- A conta de usuário que executa a instalação/upgrade/desinstalação precisa ser a de um usuário Admin local ou de domínio, que pode ser temporariamente atribuída por uma ferramenta de implementação, como o Microsoft SMS ou o Dell KACE. Não há suporte para um usuário que não é administrador mas possui privilégios elevados.
- Faça backup de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo a inserção ou a remoção de unidades externas (USB), durante a instalação.
- O Data Guardian é compatível com versões específicas do Microsoft Office 2016 e do Microsoft Office 365 Business e Business Premium. Ele é incompatível com o Office 365 Business Essentials.
- Para criptografia na nuvem, o computador deverá ter uma unidade de disco (parâmetro de letra) disponível.
- Certifique-se de que os dispositivos de destino tenham conectividade com https://yoursecurityservername.domain.com:8443/cloudweb/register e https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implantar o Data Guardian, será melhor se os dispositivos de destino ainda não tiverem as contas de armazenamento na nuvem configuradas.

  Se os usuários decidirem manter suas contas existentes, eles deverão garantir que todos os arquivos que precisem ser mantidos *descriptografados* sejam transferidos para fora do cliente de sincronização antes da instalação do Data Guardian.
- Os usuários finais deverão estar preparados para reiniciar seus computadores quando o cliente for instalado.
- O Data Guardian não interfere no comportamento dos clientes de sincronização. Portanto, os administradores e os usuários deverão se familiarizar com o modo como esses aplicativos funcionam antes de implantar o Data Guardian. Para obter mais informações, consulte suporte ao Box em https://support.box.com/home, suporte ao Dropbox em https://www.dropbox.com/help ou suporte ao OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Documentos protegidos do Office são compatíveis com Mozy, uma solução complementar do Data Guardian, bem como outros produtos de armazenamento por nuvem, e-mail e NFS.
- Se o Office 2010 estiver em execução: caso tenham sido definidas políticas para proteger documentos do Office e documentos ativados por macro, será necessário que os usuários tenham o Office 2010 Service Pack 1 ou superior (v14.0.6029 ou superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar se um service pack foi aplicado a um pacote do Microsoft Office 2010. Sem essa atualização, documentos protegidos não poderão ser acessados. Novos documentos do Office estarão desprotegidos independentemente da política, a menos que a funcionalidade varredura esteja ativada. A próxima varredura converterá documentos do Office em arquivos protegidos, mas os usuários não poderão acessá-los sem uma versão compatível do Office.
- Embora o Dell Encryption não seja exigido, se usado, o cliente de criptografia deverá ser v8.12 ou posterior.
- O Data Guardian é incompatível com a ferramenta Windows System Restore ou o Windows Insider Preview.
- O Redirecionamento de Pasta da Microsoft não é suportado no Data Guardian.
- IPv6 não é suportado com a Criptografia em nuvem.
- Verifique periodicamente dell.com/support para obter a documentação e recomendações técnicas mais recentes.

Pré-requisitos

Se ainda não estiver instalado, o instalador instalará o Microsoft Visual C++ 2015 Redistributable Package (x86 e x64).

NOTA:
Para o Windows 7 e Windows 8.1, os computadores devem estar atualizados com o Windows Update. Para obter mais informações, consulte https://support.microsoft.com/en-us/help/2919355 e https://support.microsoft.com/en-us/help/2999226.

O Microsoft .Net 4.5.2 (ou posterior) é exigido para o Data Guardian. Todos os computadores enviados da fábrica da Dell têm o .Net 4.5.2. pré-instalado. No entanto, se você não estiver instalando no hardware da Dell ou atualizando o Data Guardian em equipamentos mais antigos da Dell, você deve verificar qual versão do .Net está instalada e atualizar a versão, caso seja necessário, antes de instalar o Data Guardian para evitar falhas de upgrade/instalação. Para verificar a versão instalada do .Net, siga estas instruções no computador no qual ele será instalado: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, visite https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware

Os requisitos mínimos de hardware precisam atender às especificações mínimas do sistema operacional. A tabela a seguir detalha o hardware suportado para o cliente Windows.

Hardware Windows

- 200 MB de espaço livre em disco, dependendo do sistema operacional
- Placa de interface de rede 10/100/1000 ou Wi-Fi
- TCP/IP instalado e ativado

Se sua empresa criptografa os dados para armazenamento na nuvem, o computador deverá ter uma letra alfabética disponível para atribuir a uma unidade de disco.

Sistemas operacionais

A tabela a seguir detalha os sistemas operacionais suportados.

Sistemas operacionais Windows (32 bits e 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 Update 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro Version 1607 (Atualização de Aniversário /Redstone 1) até a versão 1803 (Spring Creators Update/Redstone 4)

NOTA:
O cliente precisa ter um desses sistemas operacionais, caso contrário ele será bloqueado. Se necessário, uma configuração em uma chave de registro permite que o administrador substitua o bloco.

Para ser compatível com o Redstone 4, é preciso fazer o upgrade do agente antes de fazer o upgrade do sistema operacional.

NOTA:
O Data Guardian não é compatível com o Windows Defender Exploit Guard (WDEG) da Microsoft no Redstone 3 e superior ou com o Kit de Ferramentas Avançado de Experiência de Mitigação (EMET) no Redstone 2 e inferior.

O Windows 7 não é suportado com a política de geolocalização para eventos de auditoria do Data Guardian.

O Data Guardian não é compatível com várias versões do Office em um computador.

Provedores de armazenamento em nuvem

A tabela a seguir detalha os provedores de armazenamento em nuvem que operam com o Data Guardian para Windows. Atualizações de provedores de armazenamento em nuvem são liberadas com frequência. A Dell recomenda testar novas versões com o Data Guardian antes de introduzi-las ao ambiente de produção.

Provedores de armazenamento em nuvem

- DropBox
- Dropbox for Business (apenas para Windows)

  NOTA:
  Dependendo da versão do Dell Server usada por sua empresa, todos os arquivos e pastas nas contas pessoais Dropbox que estão ligados a contas da empresa podem ser criptografados.
- Box

  NOTA:
  O Box Tools e o Box Edit não são suportados pelo Data Guardian. O uso do Box Tools pode causar uma condição de tela azul.
- Google Drive

  NOTA:
  Backup e Sincronização do Google não é suportado.
- OneDrive
- OneDrive for Business
- Unified OneDrive

  NOTA:
  O Unified OneDrive é um cliente de sincronização unificada para OneDrive e OneDrive for Business.

Microsoft Office

O Data Guardian é compatível com as seguintes versões do Office. No entanto, você precisa ter apenas uma versão do Office instalada.

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus: Deferred 1705, Semi-Annual 1708, and Monthly 1803

Data Guardian para Mac

A seguir, consta uma lista com hardwares suportados para o cliente Mac.

Hardware Mac

- Processador Intel Core 2 Duo, Core i3, Core i5, Core i7 ou Xeon
- 2 GB de RAM
- 10 GB de espaço livre em disco

Sistemas operacionais

A seguir, consta uma lista com os sistemas operacionais suportados.

Sistemas operacionais Mac

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

Provedores de armazenamento em nuvem

Com base nas configurações das políticas, as seguintes opções podem ser mostradas na interface do Data Guardian para Mac. O usuário não precisa fazer download nem instalar o cliente de sincronização de nuvem.

Provedores de armazenamento em nuvem

- DropBox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Aplicativo móvel para o Data Guardian

A lista abaixo apresenta os sistemas operacionais suportados no aplicativo móvel do Data Guardian.

Sistemas operacionais Android

- 4.4-4.4.4 (KitKat)
- 5.0-5.1.1 (Lollipop)
- 6.0-6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo

Sistemas operacionais iOS

- iOS 9.x
- iOS 10.x-10.3
- iOS 11-11.3

Data Guardian para Web

Para ativar o cliente Web do Data Guardian, o administrador configura uma máquina virtual para hospedar o cliente Web e se comunicar com o Dell Server v9.8 ou superior.

Os seguintes ambientes virtualizados podem ser usados para implantar o cliente Web do Data Guardian.

Ambientes virtualizados

- VMware ESXi 6.0
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/vsphere-60/index.jsp para obter mais informações
- VMware ESXi 5.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico

Ambientes virtualizados

- Consulte a página http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operacionais host compatíveis
- O hardware precisa estar em conformidade com os requisitos mínimos do VMware
- Mínimo de 4 GB de RAM para recurso dedicado de imagem
- Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações

Navegadores da Web

Você pode usar o Data Guardian com o Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Para Mac, o Safari também é compatível.

Suporte a idiomas

Esses clientes são compatíveis com interfaces de usuário multi-idiomas (MUI) e suportam os idiomas a seguir.

Suporte a idiomas

- EN - Inglês
- ES - Espanhol
- FR - Francês
- IT - Italiano
- DE - Alemão
- JA - Japonês
- KO - Coreano
- PT-BR - Português, Brasil
- PT-PT - Português, Portugal (ibérico)

3

Configurar e instalar o Data Guardian no Windows

Configurações do registro do cliente do Data Guardian

Esta seção detalha todas as configurações de registro aprovadas pelo Dell ProSupport para computadores clientes locais, independentemente do motivo para a configuração do registro. Se uma configuração de registro envolve dois produtos, ela é apresentada na lista de cada categoria.

Essas alterações no registro devem ser feitas apenas por administradores e podem não ser adequadas ou podem não funcionar em todos os cenários.

- Os níveis de registros em log podem ser aumentados para auxiliar na solução de problemas. Crie ou modifique a seguinte configuração do registro:

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  Por padrão, o nível de registro em log é definido como 0xf (15).

  Valores disponíveis:

  Off=0x0 (0)

  Critical=0x1 (1)

  Error=0x3 (3)

  Warning=0x7 (7)

  Information=0xf (15)

  Debug=0x1f (31)

- Após a instalação do Data Guardian, os usuários internos são ativados automaticamente. Se necessário, você pode modificar uma configuração do Registro para anular a ativação automática.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valor DWORD: DisableAutomaticActivation=1

  NOTA:
  Você também pode confirmar os aliases do seu domínio no Dell Server. Consulte Solução de problemas de ativação automática.

Configurar o servidor para o Data Guardian

Com base nas políticas definidas por um administrador, o Data Guardian protege os dados, por exemplo:

- Os documentos do Office armazenados localmente, compartilhados com outros usuários de várias maneiras ou armazenados em mídia removível. Estes documentos do Office podem ser protegidos: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.

- Sistemas de compartilhamento de arquivos baseados em nuvem - os computadores Windows ou dispositivos móveis capturam dados destinados ao armazenamento em nuvem, criptografam esses dados e, em seguida, os enviam para a nuvem.

Informe os usuários se a sua empresa usa o Data Guardian apenas com documentos do Office, armazenamento em nuvem, ou ambos.

Configurar o Dell Security Management Server Virtual para Data Guardian

Para configurar o Dell Security Management Server Virtual para suportar o Data Guardian, no Management Console, configure uma ou as duas políticas do Data Guardian para **Ativada**:

- *Documentos protegidos do Office* - apenas no nível da empresa
- *Criptografia de nuvem* - nível da empresa, grupos de pontos de extremidade ou pontos de extremidade

Configurar o Dell Security Management Server para Data Guardian

Para configurar o Dell Security Management Server para suportar o Data Guardian, no Management Console, configure uma ou as duas políticas do Data Guardian para **Ativada**:

- *Documentos protegidos do Office* - apenas no nível da empresa
- *Criptografia de nuvem* - nível da empresa, grupos de pontos de extremidade ou pontos de extremidade

Em seguida, Configurar o Security Server para permitir downloads de cliente de nuvem.

Configure o Security Management Server para permitir downloads do Data Guardian

Essa seção descreve as etapas necessárias para permitir que usuários façam download do cliente do Data Guardian para Windows a partir do Security Management Server.

1 No Security Management Server, navegue até o *<diretório de instalação do Security Server>\webapps\root\cloudweb\brand\dell \resources* e abra o arquivo *messages.properties* com um editor de texto.

2 Certifique-se de que as entradas estejam da seguinte forma:

```
download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe
```

3 Edite as entradas para o seguinte

```
download.deviceWin.remote.link.32=https://<URL DO SEU HOST>:<PORTA>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<URL DO SEU HOST>:<PORTA>/cloudweb/download/DataGuardian_64bit_setup.exe
```

4 Salve e feche o arquivo.

5 Vá para <diretório de instalação do Security Server> e crie uma nova pasta com o nome Download (Security Server\Download).

6 Dentro da pasta Download, crie outra nova pasta e nomeie-a de cloudweb (Security Server\Download\cloudweb).

7 Adicione os arquivos de instalação de 64 bits e 32 bits do Data Guardian à pasta cloudweb e, opcionalmente, renomeie-os, por exemplo, para DataGuardian64.exe e DataGuardian32.exe, respectivamente.

Isso é definido pelo usuário, mas deve corresponder aos nomes dos arquivos no arquivo versions.xml.

8 Reinicie o Security Server para que as alterações tenham efeito.

Configurar o Security Management Server para fazer download automático cliente Data Guardian do Windows (Opcional)

Para downloads automáticos, o arquivo versions.xml e os binários devem estar no mesmo local. O local deve ser acessível pelo cliente, por isso pode ser o IIS ou você pode usar a pasta **Security Server\Download\cloudweb** que você criou. Se estiver usando a pasta cloudweb, siga este exemplo de configuração.

1 Navegue até a pasta **Security Server\Download\cloudweb**. (consulte a etapa 6 em Configurar o Security Server para permitir downloads do cliente do Data Guardian.)

2 Crie uma pasta com o nome DataGuardianUpdate.

> **NOTA:**
> DataGuardianUpdate é usado neste exemplo, mas você pode escolher qualquer nome.

3 Coloque os arquivos executáveis atualizados na pasta DataGuardianUpdate.

4 Crie um arquivo *versions.xml* na pasta DataGuardianUpdate.

5 Abra o arquivo *versions.xml* com um editor de texto e verifique se o caminho do nome do arquivo está correto para o seu ambiente.

Exemplo:

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Versão: versão de arquivo dos executáveis atualizados

Nome do arquivo setup.exe: o nome de configuração dos executáveis é definido pelo usuário, mas deve corresponder ao nome da configuração no arquivo messages.properties (consulte a etapa 3 em Configurar o Security Server para permitir downloads do cliente do Data Guardian.)

6 Salve e feche o arquivo.

7 Adicione os binários a essa pasta.

8 Se estiver usando o IIS, reinicie o IIS.

9 Como um administrador Dell, faça login no Management Console.

10 No painel esquerdo, clique em **Populações** > **Empresa** e a guia Políticas de segurança será exibida.

11 No grupo de tecnologia do Data Guardian, clique em **Criptografia de nuvem** > **Mostrar configurações avançadas**.

12 Vá até a política *URL do servidor de atualização de software* e digite **https://<URL DO SEU HOST** > **/DataGuardianUpdate**.

> **NOTA:**
> DataGuardianUpdate é apenas um exemplo para corresponder ao exemplo acima.

13 Clique em **Salvar** para armazenar a modificação da política na fila a ser confirmada.

14 Clique em **Gerenciamento** > **Confirmar**.

15 Insira um comentário e clique em **Confirmar políticas**.

Recriar imagem de um computador com o Data Guardian instalado

Se o computador precisar ter sua imagem recriada e tiver o Data Guardian instalado, pergunte se o usuário trabalhou off-line e criou documentos protegidos do Office enquanto estava off-line. Nesse caso, as chaves off-line foram geradas para esses documentos e essas chaves não foram depositadas no Dell Server.

1 Para obter informações sobre a recuperação de chaves geradas off-line do Data Guardian que não foram depositadas no Dell Server, consulte o *Guia de Recuperação*.

2 Verifique se há uma pasta de chaves off-line antes de recriar a imagem do computador.

Quando as primeiras chaves de depósito são criadas, uma pasta do Data Guardian é adicionada a C:\Program Files\Dell. Navegue até a pasta Data Guardian > OfflineKeys. Se não houve uma pasta OfflineKeys, verifique a pasta Meus Documentos do usuário.

Desativar o EMET ou Exploit Guard da Microsoft para aplicativos gerenciados

No Windows 10, o seguinte pode ser ativado ou estar integrado no sistema operacional:

- Redstone 3 e superior - Windows Defender Exploit Guard (WDEG)
- Redstone 2 e inferior - Kit de Ferramentas Avançado de Experiência de Mitigação (EMET)

Se esses recursos estiverem ativados ou integrados, você precisa configurar as configurações para desativar estes aplicativos gerenciados para o Data Guardian:

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

Windows Defender Exploit Guard (WDEG)

Para desativar o os aplicativos gerenciados:

1. Navegue até a **Central de Segurança do Windows Defender**.
2. Clique em **Controle de navegador e aplicativo**.
3. Role até a parte inferior da tela e clique em **Explorar configurações de proteção**.
4. Selecione **Configurações do programa**.
5. Clique em **+** para adicionar cada aplicativo gerenciado listado acima.
6. Nas Propriedades de cada aplicativo gerenciado, selecione a caixa de seleção *Anular* para qualquer opção que estiver definida como *Ligar* e, em seguida, alterne a opção para **Desligar**.

   NOTA:
   Se um aplicativo gerenciado é aberto e uma caixa de diálogo indica que você deve reiniciar o .exe, reinicie-o após a conclusão dessas etapas.
7. Clique em **Aplicar**.
8. Clique em **Sim**.
   Em Configurações do programa, o aplicativo gerenciado lista as anulações com base nas opções que você alterou.

Kit de Ferramentas Avançado de Experiência de Mitigação (EMET)

Para desativar o os aplicativos gerenciados:

1. Navegue até a **Configuração do aplicativo**.
2. Nas opções **ROP Caller Check** e **Export Address Table Address Filter (EAF)**, desmarque as caixas de seleção para os aplicativos gerenciados listados acima.

Gerenciar perfis de provedor de proteção de armazenamento

O Data Guardian criptografa os arquivos dos usuários e envia eventos de auditoria para o Dell Server. Para alterar o comportamento para cada provedor de armazenamento na nuvem suportado, defina cada provedor para um desses valores:

Valor	Descrição
Proteger	Permitir conexão/provedor, criptografar os arquivos e enviar eventos de auditoria sobre atividades de pasta/arquivo.
Bloquear	Bloquear todo acesso ao provedor/conexão.
Permitir	Permitir que a conexão/provedor passe sem criptografia, mas realizar auditoria de atividades de pasta/arquivo.
Ignorar	Ignorar a proteção de conexão/provedor sem criptografia ou auditoria. Quando esse valor é definido, a pasta de provedor de armazenamento na nuvem não mostra a unidade virtual do Data Guardian no computador cliente.

Para obter mais informações, consulte o *AdminHelp*, que pode ser acessado no Remote Management Console do Dell Server.

Permitir/negar usuários da lista de acesso completo/lista negra

Você pode determinar quais usuários externos podem se registrar com o Dell Server para usar o Data Guardian. Para obter uma segurança adequada, certifique-se de configurar e gerenciar cuidadosamente essas listas.

- Um usuário interno está dentro do domínio.
- Um usuário externo é um usuário não pertencente ao domínio, uma pessoa de outra organização com a qual um usuário interno deseja compartilhar documentos sensíveis ao negócio ou um usuário interno que deseja acessar seu computador a partir de um dispositivo não pertencente ao domínio.

Para permitir que um usuário que não está no domínio da organização se registre para uso do Data Guardian:

1 No painel esquerdo do Remote Management Console, clique em **Gerenciamento > Gerenciamento de usuário externo**.

2 Clique em **Adicionar**.

3 Selecione o tipo de acesso de registro:

Lista negra - Bloqueia o registro para um usuário ou domínio. O usuário não pode abrir um documento protegido do Office ou arquivo .xen.

Lista de acesso total - Concede o acesso a registros e a todos os arquivos para um usuário ou domínio. Se um usuário ou domínio também constar na lista negra, nenhum acesso é concedido.

4 No campo Enter Domain/Email (Inserir domínio/e-mail), digite o domínio do usuário para configurar o acesso para todo o domínio ou o endereço de e-mail para configurar o acesso somente para esse usuário.

NOTA: Para usuários de dispositivos móveis externos em um ambiente de host, o e-mail deve estar em letras minúsculas.

5 Clique em **Adicionar**.

Para obter mais informações sobre o uso de lista de acesso completo/lista negra, consulte *AdminHelp*, que pode ser acessado a partir do Management Console.

Instalar o Data Guardian

Existem dois métodos para instalar o Data Guardian:

- Install Data Guardian Interactively
- Instalar o Data Guardian com a linha de comando

Os usuários do Data Guardian devem realizar as seguintes tarefas a fim de que os arquivos e pastas em seus clientes de sincronização na nuvem sejam protegidos. Após a instalação do cliente do Data Guardian, os usuários devem fazer o download de um provedor de armazenamento em nuvem:

- O administrador deve especificar qual provedor de sincronização na nuvem será usado.

  ou

- Fornecer aos usuários um link para baixar e instalar o Dropbox for Business ou o OneDrive for Business/Unified OneDrive se a sua empresa usa um desses provedores. Lembre-se de que os usuários do Dropbox for Business devem se conectar ao Dropbox for Business através do Data Guardian.

Pastas existentes com arquivos não-criptografados

Ao implantar o Data Guardian, será melhor se os dispositivos de destino ainda não tiverem a conta do provedor de armazenamento na nuvem configurada.

Se uma conta do provedor de armazenamento em nuvem estiver configurada com pastas sincronizadas com o computador local antes da instalação do Data Guardian:

- Arquivos e pastas preexistentes que sincronizam para a nuvem permanecem em texto não criptografado
- Os arquivos que você adicionar a essas pastas preexistentes permanecerão em texto não criptografado
- Arquivos que sincronizarão a partir da nuvem serão criptografados

  Se você desejar que os arquivos preexistentes sejam criptografados, navegue até a DDG VDisk virtual drive (criada quando o Data Guardian é instalado), crie uma nova subpasta no cliente de sincronização da nuvem e mova os arquivos preexistentes para essa pasta.

  ou

  Para grande conteúdo, um gerente ou administrador poderá temporariamente solicitar o Menu Gerenciar pastas.

Menu de Gerenciar pastas

Alguns gerentes ou administradores podem temporariamente precisar solucionar problemas em pastas compartilhadas por mais de um usuário. Você pode solicitar permissão do seu administrador para a opção Gerenciar pastas. Normalmente, essa é uma opção temporária.

Instalar o Data Guardian interativamente no Windows

Você precisa ser um administrador local para instalar o Data Guardian. Se os usuários irão instalar o produto, informe-os sobre a localização da mídia de instalação.

Antes de começar

Dependendo do servidor e do produto Data Guardian, faça o seguinte:

Hospedado no Dell Security Center	No local (para Dell Management Server	Criptografia na nuvem
Para lançamento futuro.	Certifique-se de que conhece o nome do Dell Security Management Server.	O computador precisa ter disponível uma letra do alfabeto para ser atribuída a uma unidade de disco.

Instalar o Data Guardian

Esteja preparado para reiniciar o computador depois que o Data Guardian for instalado.

1 Para fazer download do instalador do Data Guardian, acesse o local especificado pelo administrador.

2 Com base no sistema operacional, selecione o instalador de 32 bits ou 64 bits, normalmente **setup32.exe** ou **setup64.exe**, e copie-o para o computador local.

3 Clique duas vezes no arquivo para abrir o instalador.

4 Se for mostrado um aviso de segurança, clique em **Executar**.

5 Selecione um idioma e clique em **OK**.

6 Se aparecer uma mensagem perguntando se você quer instalar o Pacote Redistribuível do Microsoft Visual C++ 2015 ou o Microsoft .NET Framework 4.5.2 Client Profile, clique em **OK**.

7 Na página de boas-vindas, clique em **Avançar**.

8 Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.

9 Na tela Pasta de destino, clique em **Avançar** para fazer a instalação no local padrão de **C:\Arquivos de Programas\Dell\Data Guardian \.**

Em **C:**, não instale o Data Guardian nas pastas Usuários ou Windows ou na raiz de qualquer unidade. Você provocará um erro.

10 Selecione **Dell Management Server no local**:

Hospedado no Dell Security Center	Dell Management Server no local
Para lançamento futuro.	No campo *Nome do servidor de gerenciamento Dell:*, digite o nome do servidor com o qual o computador irá se comunicar, como server.domain.com. Não é necessário incluir www ou http(s). Esse dado é fornecido pelo administrador. Não desmarque a caixa de seleção *Ativar verificação da confiabilidade do SSL*, a menos que seu administrador instrua que você o faça.

11 Clique em **Avançar**.

12 Na tela Confirmar informações do servidor de gerenciamento Dell, verifique se o endereço URL do servidor está correto. O instalador acrescenta www ou http(s) e a porta. Clique em **Avançar**.

13 Na janela Tipo de gerenciamento, selecione a opção:

- Uso interno – Um usuário com endereço de e-mail no domínio da empresa.

14 Clique em **Instalar** para iniciar a instalação.

Uma janela de status mostra o andamento da instalação.

15 Clique em **Concluir** quando a tela Instalação concluída for exibida.

16 Clique em **Sim** para reiniciar.

A instalação doData Guardian está concluída.

17 Instrua os usuários a confirmarem a ativação. O ícone da bandeja do sistema do Data Guardian deve ter uma marca de seleção verde  . Dependendo da forma como o Data Guardian é implantado dentro da empresa, a ativação pode não ser imediata. Caso contrário, o usuário final precisa ativar manualmente. Em um ambiente de host, um usuário que ativa manualmente precisa reiniciar e reativar cada vez que reiniciar seu computador ou o serviço do Data Guardian. Consulte o *Data Guardian User Guide* (Guia do usuário do Data Guardian).

Instalar o Data Guardian com a linha de comando

- Parâmetros e opções de linha de comando fazem distinção entre maiúsculas e minúsculas.
- Lembre-se de cercar um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comando, com aspas como caractere de escape.
- A tabela a seguir detalha as opções disponíveis para a instalação.

Switch	Significado
/V	Passe as variáveis para o .msi dentro de setup.exe. O conteúdo deve sempre ser incluído em aspas de texto sem formatação.
/s	Modo silencioso

Opção	Significado
/QB	Caixa de diálogo de andamento com o botão **Cancelar**, solicita a reinicialização
/QB!	Caixa de diálogo de andamento sem o botão **Cancelar**, solicita a reinicialização
/QN	Sem interface do usuário

- A tabela a seguir detalha os parâmetros disponíveis para a instalação.

Parâmetros
SERVER=<ServerName> (FQDN do Dell Server para ativação)
ENTERPRISE=1 (Usuário interno)
ENABLESSLTRUST=0 (Desativar validação de confiança SSL)
REBOOT=SUPPRESS (Null permite reinicializações automáticas, SUPPRESS desativa a reinicialização)

Exemplo de linha de comando

- O exemplo a seguir instala o Data Guardian silenciosamente para um usuário interno, sem validação de confiança SSL, logs armazenados em C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

Set GPO on Domain Controller to Enable Entitlements

- Se os seus clientes forem habilitados no Dell Digital Delivery, siga estas instruções para definir o GPO no controlador de domínio para ativar a habilitação (esse pode não ser o mesmo servidor que executa o Dell Server).
- A estação de trabalho precisa ser membro do OU em que o GPO é aplicado.
- Certifique-se de que a porta de saída 443 esteja disponível para se comunicar com o Dell Server. Se a porta 443 estiver bloqueada (por qualquer motivo), o recurso de habilitação não funcionará.

1. No Controlador de domínio, para gerenciar os clientes, clique em **Start** > **Administrative Tools** > **Group Policy Management**.
2. Clique com o botão direito na OU (Organizational unit - unidade organizacional) em que a política deverá ser aplicada e selecione **Create a GPO in this domain**, and **Link it here**.
3. Digite um nome para o novo GPO, selecione "nenhum" para o Source Starter GPO (GPO de iniciador de origem) e clique em **OK**.
4. Clique com o botão direito no GPO que foi criado e selecione **Editar**.
5. O Editor de gerenciamento de política de grupo é carregado. Acesse **Computer Configuration** > **Preferences** > **Windows Settings** > **Registry**.
6. Clique com o botão direito no Registro e selecione **New** > **Registry Item**. Complete o seguinte:

   Action: Create

   Hive: HKEY_LOCAL_MACHINE

   Key Path: SOFTWARE\Dell\Dell Data Protection

   Value name: Server

   Value type: REG_SZ

   Value data: <Endereço IP do Dell Server>

7 Clique em **OK**.

8 Faça logout e depois login na estação de trabalho ou execute **gpupdate /force** para aplicar a política de grupo.

Desinstalar o Data Guardian

- Se um **usuário final** tiver uma conta de administrador local, ele mesmo poderá desinstalar o Data Guardian. Consulte o *Guia do usuário do Data Guardian* para obter informações. Esta seção descreve o processo do administrador para desinstalar o Data Guardian.

> **IMPORTANTE: Arquivos que não são do Office na DDG VDisk virtual drive**
>
> Antes de desinstalar o Data Guardian, mova todos os arquivos importantes para um local fora da DDG VDisk virtual drive. Quando o Data Guardian for desinstalado do computador de um usuário final, suas pastas e arquivos na nuvem estarão criptografados e não poderão ser lidos. Se este usuário final deixar a empresa e nenhum outro usuário compartilhar essa pasta ou arquivo, os dados ficarão ilegíveis, mas seguros (para exibir os arquivos, você poderá reinstalar o Data Guardian).
>
> Documentos do Office protegidos permanecem criptografados se você desinstalar o Data Guardian. Para descriptografar, consulte o *Guia de Recuperação > Recuperação do Data Guardian*.

Desinstalação por linha de comando

- Depois de extraído do instalador mestre, o instalador do cliente do Data Guardian pode ser encontrado em **C:\Dell \DataGuardian_XXbit_setup.exe**.
- O exemplo a seguir desinstala silenciosamente o cliente do Data Guardian.

```
setup.exe /x /s /v" /qn"
```

Reinicie o computador quando for solicitado.

Usar o Data Guardian com o Dropbox for Business

O Data Guardian com o Dropbox for Business oferece funcionalidades adicionais em relação ao Dropbox básico.

Você pode estabelecer políticas para controlar como as pastas empresariais e pessoais do Dropbox são protegidas. Se sua empresa permite contas empresariais e pessoais, os usuários finais devem entender a criptografia de cada tipo de conta. Consulte a Política para contas da empresa e pessoais.

Política para contas da empresa e pessoais

Sua empresa pode ter diretrizes que ditam se os membros da equipe podem usar contas empresariais e pessoais. Além disso, a empresa pode permitir que apenas determinados usuários tenham contas empresariais e pessoais.

> **NOTA:**
>
> Se sua empresa permite contas empresariais e pessoais, e um usuário final optar por utilizar ambas, o usuário deve entender o gerenciamento de pastas nos dois tipos de contas.

A tabela a seguir descreve a criptografia com base na configuração de política *Criptografar pastas pessoais do Dropbox*.

Criptografia	Configuração de política	Considerações de implementação
Criptografar todos os arquivos e pastas, empresariais e pessoais.	Política > Criptografar pastas pessoais do Dropbox > configurado como **Selecionado** (padrão)	Antes de o Data Guardian ser implementado, os usuários devem fazer backup dos arquivos empresariais preexistentes que estão em pastas de sincronização de armazenamento em nuvem para locais fora das pastas de sincronização.

Criptografia	Configuração de política	Considerações de implementação
		Usuários com arquivos pessoais que devam permanecer descriptografados precisam removê-los das pastas de sincronização empresariais ou desvincular contas pessoais dos clientes de sincronização empresariais. Depois da implementação do Data Guardian, arquivos e pastas da nuvem podem ser mostrados apenas em computadores ou dispositivos que estejam executando o Data Guardian. Se uma pasta pessoal for acidentalmente criptografada, consulte "Descriptografar pastas em uma conta pessoal" no Guia do usuário do Dell Data Guardian.
Criptografar todos os arquivos e pastas da conta empresarial. Permitir que arquivos e pastas da conta pessoal permaneçam descriptografados.	Política > Criptografar pastas pessoais do Dropbox > configurado como **Não selecionado**	Você pode usar a política Dropbox Encrypt Personal Folders Message (Mensagem sobre Criptografar pastas pessoais do Dropbox) opcional para mostrar uma mensagem personalizada que lembrará os usuários para **não** armazenarem arquivos da empresa em contas pessoais, pois esses arquivos não estarão protegidos. A mensagem é mostrada nessas situações: • Sempre que o usuário fizer login • Quando o usuário criar ou adicionar um novo arquivo ou pasta a uma conta pessoal do Dropbox Se você definir a política Criptografar pastas pessoais do Dropbox como Falso para um endpoint ou grupo de endpoints, as contas pessoais de todos os usuários nesses endpoints permanecerão descriptografadas.

Pastas empresariais e pessoais

Se sua empresa tem o Dropbox for Business e permite que os usuários finais tenham pastas da empresa e pessoais, pode ser que você queira executar relatórios para assegurar que todos os arquivos da empresa tenham a extensão de arquivo .xen, na eventualidade de um usuário final copiar um arquivo desprotegido confidencial para uma pasta da empresa. Consulte Solução de problemas do Data Guardian.

Exibir relatórios

As informações sobre o ambiente do Data Guardian estão disponíveis no Management Console. Selecione **Relatórios > Eventos de auditoria** para os eventos de auditoria relacionados às pastas do cliente de sincronização na nuvem e documentos protegidos do Office.

Para fins de conformidade e monitoramento de detalhes do dispositivo, Shield ou eventos de auditoria, consulte **Relatórios > Gerenciar relatórios**.

Para obter mais informações, consulte *AdminHelp*, pode ser acessado no Management Console.

Solução de problemas do Data Guardian

Usar a tela Detalhes

Você pode usar a tela *Detalhes* para solução de problemas ou por questões de suporte. Por exemplo:

- Se um usuário criar uma pasta, mas não estiver criptografando, selecione **Detalhes** > **Arquivos** > **Estado da pasta** para verificar o estado.
- Se um usuário final solicitar suporte, você poderá instruí-lo a configurar a tela Detalhes avançados e selecionar a guia **Detalhes** > **Política**. Essa guia lista que políticas estão sendo impostas.
- Ver logs para solução de problemas.

Usar a tela Detalhes aprimorados

- Enquanto você pressiona **<Ctrl><Shift>**, clique no ícone da bandeja do sistema do Data Guardian e, em seguida, selecione **Detalhes**.
- Além dos arquivos e pastas, são mostrados:

  Segurança: mostra a chave, o tipo de chave e o estado. Esse painel lista temporariamente alguns arquivos protegidos do Office até que sejam enviados para o Dell Server - o tempo depende do intervalo de sondagem.

  Auditoria: mostra módulos, ID do usuário e tipo de evento. As informações são enfileiradas nesse registro de auditoria e, em seguida, enviadas para o Dell Server em intervalos especificados. O administrador pode visualizar os **Eventos de auditoria** no painel esquerdo do Management Console para realizar a auditoria.

  Política: mostra os nomes e valores da política para sua empresa.

Mostrar arquivos de log

- Clique em **Ver log** no canto inferior esquerdo da tela Detalhes.

  Os arquivos de registro podem ser encontrados também em **C:\ProgramData\Dell\Data Guardian**.

  Os arquivos de log dos documentos protegidos do Office estão localizados na pasta Custom.xml.

Solução de problemas de ativação automática

Se o Data Guardian não ativar automaticamente para diversos usuários, você poderá alterar as Configurações do registro do cliente do Data Guardian. Você também deve verificar os aliases no Dell Server:

1. No Management Console, navegue até **Populações > Domínios** e selecione um domínio e quaisquer subdomínios.
2. Na página Detalhes do domínio, selecione a guia **Configurações**.
3. No campo *Alias*, confirme se todos os aliases estão corretos.

Fornecer direitos de gerenciamento temporário de pastas

Você pode conceder a um administrador ou usuário os direitos temporários para gerenciar pastas. Por exemplo, se o usuário carregou arquivos na nuvem antes de o Data Guardian ser instalado, você poderá fornecer direitos temporários de Gerenciamento de pasta a alguns usuários para gerenciar a criptografia em uma base de pasta a pasta dentro das pastas de cliente de sincronização.

Para fornecer direitos de gerenciamento de pasta:

1 No Management Console, clique em **Populações** > **Pontos de extremidade**.

2 Pesquise ou clique em um ponto de extremidade e, em seguida, clique na guia **Políticas de segurança**.

3 Selecione **Criptografia de nuvem** e, em seguida, clique em **Mostrar configurações avançadas**.

4 Clique na caixa de seleção ao lado de *Gerenciamento de pasta ativado* para selecionar a política.

5 Clique em **Salvar**.

6 No painel esquerdo, clique em **Gerenciamento** > **Confirmar**.

7 Insira um comentário e clique em **Confirmar políticas**.

NOTA:
A Dell recomenda que, após a criptografia das pastas ou a conclusão da solução de problemas, desmarque a caixa de seleção da política *Gerenciamento de pasta ativado* para desativar a diretiva para esse ponto de extremidade.

Para gerenciar pastas no ponto de extremidade:

1 Crie uma pasta dentro da pasta do cliente de sincronização e adicione arquivos, para que os arquivos sejam criptografados na nuvem.

2 Clique no ícone da bandeja do sistema do Data Guardian e selecione **Gerenciar pastas**.

Uma imagem em árvore de pastas sincronizadas é mostrada para cada cliente de sincronização. Todas as pastas são selecionadas por padrão. Desmarque as pastas que não deseja criptografar. Se você desmarcar uma pasta em Gerenciar pastas, uma limpeza de descriptografia descriptografará os arquivos existentes nessa pasta. Os novos arquivos nessa pasta não serão criptografados na unidade local nem na nuvem.

NOTA:
Se você arrastar um arquivo criptografado para uma pasta que está desmarcada em Gerenciar pastas na nuvem ou na unidade virtual do Data Guardian, o arquivo permanece criptografado e não é possível visualizar seu conteúdo. Além disso, se você compartilhar a pasta com outro usuário do Data Guardian que não tenha a política Gerenciar pastas ativa, os arquivos permanecerão criptografados para ele e ele não conseguirá visualizar o conteúdo.

3 Para criptografar uma pasta preexistente, ative manualmente a criptografia dessa pasta. Os arquivos são criptografados durante a sincronização dos arquivos na nuvem.

Frequently Asked Questions

FAQs de gerenciamento de pastas

Pergunta

Tenho uma pasta com arquivos que compartilhei com outro usuário. Na bandeja de sistema, eu usei o utilitário do **Data Guardian > Gerenciar pastas** para descriptografar o conteúdo da pasta. Recentemente, meus arquivos foram criptografados na nuvem, novamente. Essa pasta não mostra mais o utilitário Gerenciar pastas, de modo que não posso mais descriptografar esses arquivos na nuvem.

Resposta

Uma ID de chave de criptografia está associada a uma pasta baseada no primeiro usuário que adicionar um arquivo a essa pasta. Se um usuário criar uma pasta e não adicionar qualquer arquivo, sua chave não estará associada a essa pasta. O usuário cuja ID de chave de criptografia tiver sido configurada na pasta é o único que poderá ver a pasta no utilitário Gerenciar pastas. Se o usuário cujo ID de chave de criptografia estiver configurado na pasta desmarcá-la no utilitário Gerenciar pastas e compartilhá-la com outro usuário do Data Guardian, o Data Guardian do segundo usuário irá criptografar novamente o conteúdo.

Solução

1 Criar uma nova pasta.

2 Mova todos os arquivos que devem ser criptografados para a nova pasta.

3 Na bandeja de sistema, use novamente o utilitário do **Dell Data Guardian** > **Gerenciar pastas** para decriptografar esses arquivos.

NOTA:
Se você descriptografar o conteúdo de uma pasta que é compartilhado com outro usuário do Data Guardian, o Data Guardian do outro usuário fará com que a política o criptografe. A melhor prática é usar o utilitário Gerenciar pastas para descriptografar apenas os arquivos que não são compartilhados com outros usuários do Data Guardian.

Pergunta

Estou fazendo a sincronização para uma pasta descriptografada que eu desmarquei usando o utilitário Gerenciador de pastas. Entretanto, quando tento fazer upload da pasta através do navegador da Web, só consigo fazer upload de arquivos criptografados.

Resposta

O Data Guardian não foi projetado para pesquisar ativamente as pastas na nuvem. Com pastas decriptografadas, o Data Guardian pode sincronizar através do cliente de sincronização porque ele controla o ambiente. É necessário que os arquivos que passam pelo navegador da Web sejam criptografados.

Solução

Adicionar arquivos à pasta de sincronização

Pergunta

Eu desinstalei recentemente o meu sistema de compartilhamento de arquivos baseado em nuvem do meu computador, mas quando eu abri o utilitário Gerenciar Pastas, um dos clientes de sincronização ainda estava aparecendo como uma opção.

Resposta

O Data Guardian não monitora a instalação ou desinstalação de softwares provenientes de terceiros. Essas opções ainda aparecem porque, por projeto, quando esses clientes são desinstalados, eles não removem os seus arquivos existentes. Esses arquivos serão protegidos pelo Data Guardian mesmo que o cliente de sincronização não esteja mais instalado.

Solução

Para remover a opção do cliente de sincronização desinstalada do utilitário Gerenciar pastas, mova todas as pastas/arquivos que você deseja manter fora da pasta de sincronização e exclua a pasta. Depois de excluir a pasta, ela não será mais listada no utilitário Gerenciamento de pasta.

Perguntas frequentes sobre assuntos diversos

Pergunta

Um usuário tem o Data Guardian com documentos protegidos do Office e não pode copiar ou colar.

Resposta

Para o Data Guardian, algumas funcionalidades são processadas através do systray. Verifique se o usuário modificou o systray.

Solução

Devem ser usadas as configurações padrão do systray. O usuário deve manter as configurações padrão do systray.

Pergunta

Eu alterei a política **Ofuscar nomes de arquivo** do Guid para Apenas a extensão. Entretanto, as pastas que antes eu usava para sincronização ainda estão criptografando esses arquivos para o outro formato com nomes de arquivo de Guid. Por quê?

Resposta

Quando uma política é alterada no Security Management Server/Security Management Server Virtual, o Data Guardian mantém a política anterior dessa pasta. Todas as novas pastas criadas terão a nova política aplicada e criptografarão no formato **Apenas a extensão**.

Solução

Para reaplicar o formato **Apenas a extensão** aos arquivos antigos, recorte e cole em uma nova pasta que tenha a nova política aplicada.

Configurar e instalar o Data Guardian no Mac

O Data Guardian para Mac é projetado para compartilhar arquivos dentro de provedores de criptografia em nuvem. No entanto, se políticas de Documentos protegidos do Office forem ativadas para Macs e se o arquivo for salvo pelo usuário no Mac local, a auditoria e a rastreabilidade de todos os arquivos serão perdidas. Caso sua organização precise de uma rigorosa auditoria e rastreabilidade de arquivos, defina a política *Permitir ativação do Data Guardian no Mac* como **Não selecionado** para impedir que o Data Guardian seja ativado em Macs.

Tarefas do servidor

Pré-requisitos

Antes de realizar essas tarefas, confirme o seguinte:

- Instale o Dell Server e seus componentes. Veja uma dessas opções:
  - *Security Management Server Installation and Migration Guide (Guia de instalação e migração do Servidor de gerenciamento de segurança)*
  - *Security Management Server Virtual Quick Start Guide and Installation Guide (Guia de instalação e de início rápido do Servidor de gerenciamento de segurança virtual)*
- No Management Console, atribua uma função de administrador Dell apropriada.

Políticas

Por padrão, o Data Guardian criptografa os arquivos dos usuários e envia eventos de auditoria ao Security Management Server Virtual. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Security Management Server Virtual).

Se quiser que os eventos de auditoria incluam dados de localização geográfica, é preciso ativar o Wi-Fi. Para obter mais informações sobre localização geográfica e eventos de auditoria, consulte *AdminHelp*.

Para alterar o comportamento padrão de cada provedor de armazenamento em nuvem suportado, configure a política de *Provedores de proteção de armazenamento na nuvem*. Caso sua empresa prefira um provedor de armazenamento em nuvem específico, defina essa política como **Bloquear** para outros provedores. Para obter mais informações sobre políticas, consulte a *AdminHelp*, que pode ser acessada no Management Console.

NOTA:
A opção Desviar dessa política é para Windows. Se a opção Desviar for selecionada para Mac, ela será mostrada para o usuário final como Permitir.

Configurar o Security Server para permitir downloads de cliente de nuvem

Antes de realizar essas tarefas, confirme o seguinte:

- Instale o Dell Server e seus componentes. Veja uma dessas opções:
  - *Guia de instalação e migração do Security Management Server*
  - *Guia de instalação e de início rápido do Security Management Server Virtual*
- No Management Console, atribua uma função de administrador Dell apropriada.

Security Management Server

1 No Security Management Server, vá até <diretório de instalação do Security Server>\webapps\cloudweb\brand\dell\resources\
2 Abra o arquivo **messages.properties** com um editor de texto.
3 Verifique se as entradas são as seguintes:
Para a instalação **local**:

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Para a instalação **remota**:

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[NomeDaMáquina:EndereçoIP]:[porta]/caminho/
nome_do_arquivo.dmg
```

4 Salve e feche os arquivos.
5 Vá para <diretório de instalação do Security Server> e crie uma pasta com o nome Download (Security Server\Download).
6 Na pasta Download, crie uma pasta CloudWeb (Security Server\Download\CloudWeb).
7 Adicione os instaladores do Dell Data Guardian a essa pasta.

Virtual Edition: instale manualmente outra versão do cliente de nuvem

Nenhuma ação é necessária para permitir que os usuários façam download do instalador mais recente do Dell Data Guardian. O instalador mais recente está pré-instalado no servidor de segurança Security Management Server Virtual.

Para instalar manualmente outra versão do instalador do Data Guardian no Security Management Server Virtual Security Server, atualize o arquivo message.properties.

1 Vá para:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Abra o arquivo **messages.properties** com um editor de texto.
Para a instalação **local**:

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Para a instalação **remota**:

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[NomeDaMáquina:EndereçoIP]:[porta]/caminho/
nome_do_arquivo.dmg
```

3 Salve e feche os arquivos.

4 Copie os arquivos para /opt/dell/server/security-server/download/cloudweb.

5 Adicione os instaladores do Data Guardian a essa pasta.

Permitir/negar usuários da lista de acesso completo/lista negra

As entradas da lista de acesso completo e da lista negra determinam quais usuários podem se registrar no Dell Server para usar o Data Guardian.

Lista de acesso completo

A lista de acesso completo permite que determinados usuários ou grupos de usuários se registrem no Dell Server e usem o Data Guardian.

Usuários externos precisam ser colocados na lista de acesso completo para permitir o registro. Veja os exemplos a seguir para permitir que os usuários se inscrevam:

Tipo de usuário	Incluir
Todos os endereços de e-mail em organização.com	`organization.com`
Um usuário específico	`jdoe@organization.com`
Todos os usuários do Gmail	`gmail.com`

Lista negra

A lista negra impede que usuários ou grupos específicos se registrem no Dell Server e usem o Data Guardian. Os usuários cujos endereços de e-mail forem inseridos na lista negra receberão uma mensagem informando-os que não podem se registrar no Data Guardian.

NOTA:
Se um usuário já estiver registrado, essa lista **não** o impede de utilizar o Data Guardian.

Você pode usar a lista negra para excluir usuários específicos que são membros de grupos aprovados na lista de acesso completo. Além disso, é possível colocar domínios inteiros na lista negra, o que impedirá que qualquer pessoa com um endereço de e-mail nesse domínio se registre. Veja os exemplos a seguir para impedir que um usuário ou grupo se registre no Dell Server:

Tipo de usuário	Incluir
Todos os endereços de e-mail em organização.com	`organization.com`
Um usuário específico e seu endereço de e-mail	`jdoe@organization.com`
Todos os usuários do Gmail	`gmail.com`

Para modificar a lista de acesso completo/lista negra, siga estas instruções:

1 No painel esquerdo do Remote Management Console, clique em **Gerenciamento > Gerenciamento de usuário externo**.

2 Clique em **Adicionar**.

3 Selecione o tipo de acesso de registro:

Lista negra - Bloqueia o registro para um usuário ou domínio. O usuário não pode abrir um documento protegido do Office ou arquivo .xen.

Lista de acesso total - Concede o acesso a registros e a todos os arquivos para um usuário ou domínio. Se um usuário ou domínio também constar na lista negra, nenhum acesso é concedido.

4 No campo Enter Domain/Email (Inserir domínio/e-mail), digite o domínio do usuário para configurar o acesso para todo o domínio ou o endereço de e-mail para configurar o acesso somente para esse usuário.

5 Clique em **Adicionar**.

Para obter mais informações sobre o uso de lista de acesso completo/lista negra, consulte *AdminHelp*, acessível no Remote Management Console do Dell Server.

Um usuário externo pode solicitar acesso à chave para um arquivo protegido a um usuário interno. Se o usuário interno não estiver disponível, é possível usar o Remote Management Console para aprovar ou negar o acesso.

1 Selecione **Gerenciamento > Gerenciamento de solicitação de chave**.

2 Para obter mais informações, selecione **?** (Ajuda).

Tarefas de cliente

Pré-requisitos

- Verifique se os dispositivos de destino têm conectividade com:
  - https://nome_do_seu_securityserver.domínio.com:8443/cloudweb/register
  - https://nome_do_seu_securityserver.domínio.com:8443/cloudweb
- Confirme que o usuário que está executando a instalação tem uma conta de administrador local para a instalação.
- Se estiver instalando por linha de comando, verifique se você tem o nome de domínio totalmente qualificado do Security Server no qual os usuários serão ativados.

Práticas recomendadas

Durante a implementação, siga as práticas recomendadas de TI. Isso inclui, sem limitações:

- Ambientes de teste controlados para testes iniciais
- Implementações escalonadas para os usuários

Instalar o cliente

Neste momento, os usuários que foram adicionados à lista branca podem se inscrever em: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Após se inscrever, o usuário receberá um e-mail direcionando-o a https://yoursecurityservername.domain.com:8443/cloudweb para fazer login e o download do cliente adequado.

A instalação do cliente Mac é opcional para os administradores, pois os usuários finais normalmente instalarão o cliente Mac sozinhos (após o registro) a partir do site https://yoursecurityservername.domain.com:8443/cloudweb.

Entretanto, você pode instalar o cliente Mac caso sua organização exija. Instale o cliente Data Guardian por meio da interface do usuário ou pela linha de comando usando qualquer tecnologia push disponível para a sua organização. A inscrição e a ativação pelo usuário final ainda são necessárias.

Atualização de versões anteriores do Cloud Edition

Se uma empresa tiver uma versão anterior do Cloud Edition e fizer a atualização para o Data Guardian, a versão anterior do Cloud Edition é removida.

NOTA:
Se a empresa fizer a atualização do Cloud Edition para o Data Guardian, os usuários precisam autenticar e vincular novamente o Data Guardian ao provedor de armazenamento em nuvem deles. Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

Opções de instalação

Para instalar/fazer upgrade do cliente, selecione uma das opções a seguir:

- Instalação interativa - Esse é o método mais fácil para instalar o Data Guardian para Mac. Entretanto, use este método apenas se você planeja instalar o cliente em um computador de cada vez.

  ou

- Instalação por linha de comando - Para esse método avançado de instalação, os administradores devem ter experiência em sintaxe de linha de comando. Este método pode ser usado para uma instalação com scripts, arquivos de lotes ou qualquer outra tecnologia push disponível para sua organização.

Instalação interativa

1. Para o cliente Data Guardian, localize o instalador em **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Use o arquivo **.pkg** dentro do DDPSL-Explorer-0.x.x.xxxx.dmg para instalar ou atualizar. Você pode usar uma instalação com scripts, arquivos de lotes ou qualquer outra tecnologia push disponível para sua organização.
3. Clique duas vezes no pacote **Dell-Data-Guardian-x.x.x**.
4. Clique em **Continuar**.
5. Na janela Introdução, clique em **Continuar**.
6. Na janela Contrato de Licença de Software, clique em **Continuar**.
7. Clique em **Concordo** para continuar.
8. Na janela Tipo de configuração, selecione **Dell Management Server no local**.

   NOTA:
   Hosted Dell Security Center é para um lançamento futuro.

9. Na janela Tipo de instalação, faça um dos seguintes:
   - Clique em **Instalar** e, em seguida, vá para a etapa 9.
   - Clique em **Alterar local de instalação**.
     1. Na janela Seleção de destino, selecione todos ou um único usuário.
     2. Clique em **Continuar**.
     3. Clique em **Instalar** e, em seguida, vá para a etapa 9
10. Na caixa de diálogo, digite o nome de usuário e a senha, e clique em **Instalar software**.
11. Na janela Resumo, clique em **Fechar**.
12. Consulte Ativação do usuário final.

    NOTA:
    Se a empresa fizer a atualização do Cloud Edition para o Data Guardian, os usuários precisam autenticar e vincular novamente o Data Guardian ao provedor de armazenamento em nuvem deles. Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

13. Feche a janela .dmg para abrir o Localizador.

Instalação por linha de comando

1. Monte o arquivo .dmg.

2 Execute a instalação do pacote por linha de comando usando o comando installer:

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```

3 Instrua os usuários a ativar o Data Guardian. Consulte Ativação do usuário final.

Ativação do usuário final

Depois de abrir o Dell Data Guardian no Mac pela primeira vez, siga estas etapas:

1 No Finder, selecione **Aplicativos**, e clique duas vezes em **Dell Data Guardian**.
2 Quando a janela Dell Server se abrir, digite o endereço do Dell Server e clique em **Salvar**.

A janela Credenciais será aberta.

3 Digite o seu endereço de e-mail de domínio e a sua senha de domínio.
4 Clique em **Login** para ativar o Dell Data Guardian.

Quando o aplicativo Dell Data Guardian abrir e a ativação for concluída com sucesso, o nome do provedor de armazenamento na nuvem é exibido no painel esquerdo.

Se uma empresa desejar que todos os usuários colaborem usando o mesmo provedor na nuvem, o administrador pode configurar uma política para permitir apenas tal provedor e bloquear que outros sejam exibidos.

Se a autenticação do aplicativo Dell Data Guardian for revogada ou vencer, o nome do provedor de armazenamento em nuvem aparecerá esmaecido.

5 No painel esquerdo, selecione o provedor de armazenamento em nuvem.

Uma janela será aberta solicitando suas credenciais. Quando autenticado, o nome de fornecedor do armazenamento em nuvem é ativado.

6 Para obter mais informações sobre a autenticação, consulte a ajuda on-line do Dell Data Guardian.

Desinstalar o Data Guardian

Esta seção descreve o processo do administrador para desinstalar o Data Guardian. Você precisa ter uma conta de administrador local para fazer a desinstalação. Se um usuário final tiver uma conta de administrador local, ele mesmo poderá desinstalar o Data Guardian para Mac.

Siga um dos procedimentos abaixo para remover o Data Guardian:

Finder

1 Enquanto pressiona a tecla <opção>, selecione **Ir** na barra de menu.
2 Abra a pasta **~/Library/Application Support/Dell**.
3 Clique com o botão direito na pasta **DellDataGuardian** e selecione **Mover para a Lixeira**.
4 Na opção **Ir** na barra de menu, abra a pasta Aplicativos e mova o aplicativo **Data Guardian** para a Lixeira.
5 Clique em **OK**.
6 Se solicitado, digite a senha de administrador.

Terminal

Você pode ter o Data Guardian em um ou em ambos os locais a seguir.

1 Use estes comandos:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Remova a pasta **DellDataGuardian.**

5

Configurar e instalar o Data Guardian para o cliente Web

Esse cliente Web permite que os usuários vejam um documento protegido do Office ou um arquivo .xen sem instalar o cliente do Data Guardian. Como regra geral, a Dell recomenda a instalação do Security Management Server ou do Security Management Server Virtual primeiro.

Fazer download do arquivo OVA

Na instalação inicial, o Data-Guardian-Web é fornecido como um arquivo OVA (Open Virtual Application), um aplicativo virtual aberto usado para oferecer softwares que são executados em uma máquina virtual.

Para fazer download do arquivo OVA:

1 Navegue até a página de suporte ao produto do Data Guardian.
2 Clique em **Drivers e downloads**.
3 Ao lado de "Ver todas as atualizações disponíveis para <versão do SO>," clique em **Alterar SO** e selecione uma das opções a seguir: **VMware ESXi 6.0** ou **VMware ESXi 5.5**.
4 Em “Ver por:”, selecione **Exibir todos**.
5 Em Dell Data Security, selecione **Download**.

Instalar o Data Guardian para Web

Instalar e configurar o Data-Guardian-Web

Antes de começar, verifique se todos os requisitos de ambiente virtual e do sistema são atendidos.

1 Localize os arquivos do Data Guardian na mídia de instalação e clique duas vezes em **Data-Guardian-Web-1.x.x.ova** para importar para o VMware.
2 Ative o Data-Guardian-Web.
3 Selecione o idioma para o contrato de licença e selecione **Mostrar EULA**.
4 Leia o contrato e selecione **Aceitar EULA**.
5 Se houver uma atualização disponível, selecione **Aceitar**.
6 No prompt de alteração de senha padrão, selecione **Sim**.
7 Na tela *Definir senha do ddguser*, digite a senha (padrão) atual, **ddguser**, em seguida insira uma senha única, digite novamente a senha única e selecione **OK**.

   As senhas precisam conter o seguinte:

   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 caractere especial

8 Repita a etapa anterior para as contas *ddgconsole* e *ddgsupport*.

NOTA:
Para manter a senha padrão, igual ao nome, clique em **Cancelar**. Para modificar a senha, digite **ddgconsole** ou **ddgsupport** no campo Senha atual.

9 Na caixa de diálogo *Configurar nome de host*, use a tecla Backspace para remover o nome de host padrão. Digite um nome de host FQDN e selecione **OK**.

10 Se você tiver múltiplos nós e um balanceador de carga, digite um nome de host para o Balanceador de carga.

11 Na diálogo *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.

- (Padrão) Usar o DHCP
- (Recomendado) No campo Usar DHCP, pressione a barra de espaço para remover o X e inserir manualmente esses endereços, conforme aplicável: IP estático, Máscara de rede, Gateway padrão, Servidor de DNS 1, Servidor de DNS 2, Servidor de DNS 3.

NOTA:
Quando um IP estático é usado, é necessário também criar uma entrada de host no servidor DNS.

12 Quando a tela scp for exibida, não clique em OK. Você precisa adicionar primeiro os arquivos .cer e .key para o aplicativo ou extrair o arquivo .pfx ou .p7b do CA. Consulte Use a ferramenta WinSCP.

NOTA:
Se clicar em OK na tela scp antes de os extrair, você deve reiniciar o Data-Guardian-Web e navegar até a caixa de diálogo *Definir as configurações de rede*.

Use a ferramenta WinSCP

No Windows, use a conta do ddgconsole para scp para o arquivo do certificado SSL, o arquivo da chave do SSL e o arquivo da chave do SSL.

1 No Windows, abra a ferramenta WinSCP.

2 Na página da ferramenta WinSCP, digite o nome do host.

3 Digite o nome de usuário ddgconsole padrão e a senha padrão (ou sua senha e e nome de usuário modificados).

4 Clique em **Fazer login**.

5 Arraste o certificado e chave o arquivo .pfx, ou .p7b a partir de sua unidade local para o diretório **opt/dell/files**.

6 Se você adicionou um arquivo .pfx ou .p7b, digite uma senha quando solicitado. O certificado e chave são extraídos do CA e adicionados a **apache2/ssl/folder**.

Opcionalmente, em vez de arrastar o arquivo .pfx ou .p7b, você pode extrair o certificado manualmente. Segue um código de exemplo:

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

Segue um código de exemplo para extrair a chave privada do arquivo .pfx:

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 Volte para a tela scp do Console de Administração.

Administration Console

Na tela scp do Console de Administração:

1 Clique em **OK**. A tela de *Instalação de certificado de proxy reverso Apache2* é exibida, listando o certificado.

2 Selecione um certificado e clique em **Enter**.

3 Execute um destes processos:

- Se você adicionou uma chave na ferramenta WinSCP, selecione a chave na tela seguinte e pressione **Enter**.
- Se você digitou uma senha na ferramenta WinSCP para um arquivo .pfx ou .p7b, digite a senha quando solicitado e clique em **OK**.

4 Na tela Configurar Dell Server, digite o nome de host do servidor e clique em **OK**. Uma caixa de diálogo é exibida, listando um URL para usar durante o provisionamento. O URL está no seguinte formato: **https://node.domain.com/edap-admin-ui/provision_node**.

NOTA:
node.domain.com é o nome digitado em *Configurar nome de host*. O URL aponta para esse nó.

5 Abra um navegador e digite esse URL.

6 Quando a página de provisionamento do nó do Dell Data Guardian abrir, clique em **Iniciar provisionamento do nó**.

7 Na página de login, digite o email de domínio e a senha e clique em **Fazer login**. A caixa de diálogo do Dell Data Guardian indica que o provisionamento foi bem-sucedido.

8 Volte para a tela do Console de Administração que listou seu URL e clique em **OK**. O servidor de aplicativos é reiniciado e o Administrator Console > Menu principal é aberto.

Tarefas adicionais:

- Forneça o URL aos usuários internos para permitir que acessem o cliente Web do Data Guardian.
  - Para um único nó, o URL é neste formato: **https://nodename/**, onde nodename reflete o nome de host digitado na tela *Configurar nome de host*.
  - Para vários nós, o URL é neste formato: **https://loadBalancerName/**, onde nodename reflete o nome de host do balanceador de carga digitado na tela *Configurar nome de host*.
- Para acessar o servidor no futuro a fim de obter atualizações para esta máquina virtual ou para verificar os logs, você precisa habilitar o SSH para esta máquina virtual. Selecione **Configuração básica > Configurações de SSH** para ativar o SSH para um usuário ddgsupport.
- No Management Console, se você modificar alguma política de portal Web baseada em nó, você precisará reinicializar o dispositivo. Consulte Reinicializar o dispositivo. Após a reinicialização, você precisa fazer login com as credenciais do ddguser.

Abrir o Management Console

Abra o Management Console no endereço: https://server.domain.com:8443/webui/

As credenciais padrão são **superadmin/changeit**.

Os seguintes navegadores da Web são compatíveis para acessar o Management Console:

- Internet Explorer 11.x ou posterior
- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior
- Safari

Tarefas básicas de configuração do terminal do Data Guardian

As tarefas de configuração básica são acessadas pelo menu principal.

Alterar Nome de host

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o .

1 No menu *Configuração básica*, selecione **Nome do host**.

2 Use a tecla de espaço para remover o nome do host Data-Guardian-Web existente, substitua-o por um novo nome de host e selecione **OK**.

Alterar configurações de rede

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o .

1 No menu *Configuração básica*, selecione **Rede**.
2 Na tela *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.
   - (Padrão) Usar o DHCP (IPv4).
   - (Recomendado) No campo Usar DHCP, pressione a barra de espaço para remover o X e digite esses endereços manualmente, conforme necessário:

     IP estático

     Máscara de rede

     Gateway padrão

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

     IPv6 ou IPv4 podem ser selecionados para uma configuração estática.

   NOTA:
   Ao usar um IP estático, você precisa criar uma entrada de host no servidor DNS.

Alterar senhas de usuário

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o .

Você pode alterar senhas para esses usuários:

- ddguser (Administrador do terminal) - Este usuário tem acesso ao terminal e aos menus do Data Guardian do .
- ddgconsole (acesso shell) - Este usuário tem acesso shell ao Data Guardian do . O acesso ao shell está disponível para um administrador de rede a fim de verificar e solucionar problemas de conectividade de rede.
- ddgsupport (Administrador do Dell ProSupport) – Este usuário existe apenas para uso do Dell ProSupport. Para fins de segurança, você controla a senha para esta conta.

1 No menu *Configuração básica*, selecione **Alterar senhas de usuário**.
2 Na tela *Alterar senhas de usuário*, selecione a senha de usuário que será alterada e selecione **Entrar**.
3 Na tela *Definir senha*, insira a senha atual, insira a nova senha, insira a nova senha de novo e selecione **OK**.
   As senhas precisam conter o seguinte:

   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 caractere especial

   NOTA: Para escolher diferentes contas de usuário, use a "barra de espaço" no teclado para mostrar a lista de seleção.

Habilitar o SSH

Essa tarefa pode ser executada a qualquer momento. Não é necessário começar a usar o .

Você pode ativar o SSH para o login do administrador de suporte, acesso ao shell e a interface de linha de comando do terminal.

1 No menu *Configuração básica*, selecione **SSH**.
2 Selecione o usuário para o qual deseja habilitar o SSH, pressione a barra de espaço para inserir um **X** e selecione **OK**.

Iniciar ou parar serviços

Execute esta tarefa somente se for necessário.

1 Para iniciar ou parar simultaneamente todos os serviços, no menu *Configuração básica*, selecione **Iniciar aplicativo** ou **Parar aplicativo**.
2 Na janela de confirmação, selecione Sim.

NOTA: As alterações no estado do servidor poderão levar até dois minutos para serem concluídas.

Reinicializar o dispositivo

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, selecione **Reinicializar o dispositivo**.
2 Na janela de confirmação, selecione Sim.
3 Depois de reiniciar, faça login no Data Guardian.

Desligar o dispositivo

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, desça e selecione **Encerrar dispositivo**.
2 Na janela de confirmação, selecione Sim.
3 Depois de reiniciar, faça login no Data Guardian.

Tarefas do administrador

Definir ou alterar o idioma do terminal

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu principal, selecione **Definir idioma**.
2 Use as teclas de seta para selecionar o idioma preferencial.

Gerar um log de instantâneos do sistema

Para gerar um log de instantâneo do sistema para o Dell ProSupport, no menu principal, selecione **Ferramentas de suporte**.

1 No menu *Ferramentas de suporte*, selecione **Gerar log de instantâneo de sistema**.
2 Na indicação que o arquivo é criada, selecione **OK**.