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 a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

Guia do Administrador para Windows, Mac, Dispositivos móveis e Web

2018 - 08

Rev. A01

Índice

1

Introdução

Todas as informações sobre políticas e as respetivas descrições podem ser encontradas em AdminHelp.

Antes de começar

1 Instale o Dell Server antes de implementar os clientes. Localize o guia correto como mostrado abaixo, siga as instruções e, em seguida, volte a este guia.

- *Guia de instalação e migração doSecurity Management Server*
- *Guia de instalação e guia de início rápido do Security Management Server Virtual*
- Certifique-se de que as políticas foram definidas da forma pretendida. Navegue no AdminHelp, disponível através de **?** no canto superior direito do ecrã. O AdminHelp é uma ajuda ao nível da página concebida para o ajudar a definir e modificar a política e a compreender as suas opções relativamente ao seu Dell Server.

2 Leia atentamente o capítulo Requisitos deste documento.

3 Implemente os clientes para utilizadores.

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

Para números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

Requisitos

Dell Server

O Data Guardian para Windows, Mac e Mobile requer o Security Management Server ou o Security Management Server Virtual v9.6 ou posterior. O cliente Web do Data Guardian requer o Security Management Server ou o Security Management Server Virtual v9.8 ou posterior. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Security Management Server Virtual).

Data Guardian para Windows

- Durante a implementação, devem ser seguidas as melhores práticas de TI. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.
- A conta de utilizador que realiza a instalação/atualização/desinstalação deve ser um utilizador administrador local ou de domínio, que poderá ser atribuído temporariamente por uma ferramenta de implementação, como o Microsoft SMS ou Dell KACE. Não são suportados utilizadores não administradores com privilégios elevados.
- Realize uma cópia de segurança de todos os dados importantes antes de iniciar a instalação/desinstalação.
- Não realize alterações no computador, incluindo inserir ou remover unidades externas (USB) durante a instalação.
- O Data Guardian é compatível com versões específicas do Microsoft Office 2016 e também do Microsoft Office 365 Empresas e Empresas - Versão Premium. Não é compatível com o Office 365 Empresas - Versão Essentials.
- Para encriptação na nuvem, o computador deve ter uma (letra) unidade de disco atribuível disponível.
- Certifique-se de que os dispositivos de destino estão ligados a https://yoursecurityservername.domain.com:8443/cloudweb/register https://yoursecurityservername.domain.com:8443/cloudweb
- Antes de implementar o Data Guardian, é preferível que os dispositivos de destino não tenham ainda contas de armazenamento na nuvem configuradas.

  Se os utilizadores decidirem manter as respetivas contas existentes, devem certificar-se de que quaisquer ficheiros que devam permanecer *sem encriptação* são retirados do cliente de sincronização antes de instalar o Data Guardian.
- Os utilizadores devem estar preparados para reiniciarem os respetivos computadores depois de instalarem o cliente.
- O Data Guardian não interfere no comportamento de clientes de sincronização. Por conseguinte, os administradores e utilizadores devem familiarizar-se com o funcionamento destas aplicações antes de implementarem o Data Guardian. Para obter mais informações, consulte o apoio técnico do Box em https://support.box.com/home, o apoio técnico do Dropbox em https://www.dropbox.com/help ou o apoio técnico do OneDrive em http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Os documentos do Office protegidos são suportados pelo Mozy, uma solução complementar do Data Guardian, bem como por outros produtos de armazenamento em nuvem, e-mail e NFS.
- Se estiver em execução o Office 2010: caso tenham sido definidas políticas para proteger documentos do Office e documentos com permissão para macros, os utilizadores têm de ter o Service Pack 1 do Office 2010 ou superior (v14.0.6029 ou superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar se foi aplicado um service pack a uma suite do Microsoft Office 2010. Sem esta atualização, não é possível aceder a documentos protegidos. Os novos documentos do Office estão desprotegidos, independentemente da política, exceto se a funcionalidade de varrimento estiver ativada. O próximo varrimento converte os documentos do Office em ficheiros protegidos, mas os utilizadores não podem aceder aos mesmos sem uma versão compatível do Office.
- Embora a Dell Encryption não seja necessária, se for utilizada, o cliente de encriptação deve ser v8.12 ou posterior.
- O Data Guardian não é compatível com a ferramenta de restauro do sistema Windows nem com o Windows Insider Preview.
- O Redirecionamento de Pastas da Microsoft não é suportado com o Data Guardian.
- O protocolo IPv6 não é suportado com Cloud Encryption.
- Certifique-se de que verifica periodicamente a página dell.com/support para procurar a documentação e os avisos técnicos mais atuais.

Pré-requisitos

Se ainda não estiver instalado, o programa de instalação instala o Pacote Redistribuível do Microsoft Visual C++ 2015 (x86 e x64).

NOTA:
No 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.

É necessário Microsoft .Net 4.5.2 (ou posterior) para o Data Guardian. Todos os computadores enviados da fábrica da Dell estão previamente equipados com o .Net 4.5.2. No entanto, se não instalar no hardware Dell ou se atualizar o Data Guardian num hardware Dell mais antigo, deve verificar qual a versão do .Net instalada e atualizar a versão antes de instalar o Data Guardian para impedir falhas na instalação/atualização. Para verificar a versão instalada do .Net, siga estas instruções no computador onde pretende efetuar a instalação: ttp://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar o Microsoft .Net Framework 4.5.2, aceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware

Os requisitos mínimos de hardware necessitam atender as especificações mínimas do sistema operativo. A tabela seguinte apresenta o hardware suportado para o cliente Windows.

Hardware Windows

- 200 MB de espaço livre no disco, dependendo do sistema operativo
- Placa de rede 10/100/1000 ou Wi-Fi
- TCP/IP instalado e ativado

Se o seu Enterprise encriptar os dados para o armazenamento na nuvem, o seu computador tem de ter uma letra do alfabeto disponível para atribuir a um disco rígido.

Sistemas operativos

A tabela seguinte apresenta os sistemas operativos suportados.

Sistemas operativos Windows (32 bits e 64 bits)

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

NOTA:
O cliente tem de dispor de um dos seguintes sistemas operativos ou será bloqueado. Se necessário, uma definição numa chave de registo permite ao administrador ultrapassar o bloqueio.

Para obter suporte para o Redstone 4, tem de atualizar o agente antes de atualizar o sistema operativo.

NOTA:

O Data Guardian não é compatível com o Windows Defender Exploit Guard (WDEG) da Microsoft no Redstone 3 e posterior ou com o Enhanced Mitigation Experience Toolkit (EMET) no Redstone 2 e anterior.

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

O Data Guardian não suporta várias versões do Office num computador.

Fornecedores de armazenamento na nuvem

A tabela seguinte detalha os fornecedores de armazenamento na nuvem que funcionam com o Data Guardian para Windows. As atualizações do fornecedor de armazenamento na nuvem são lançadas frequentemente. A Dell recomenda que proceda a testes das novas versões com o Data Guardian antes de as incorporar no ambiente de produção.

Fornecedores de armazenamento na nuvem

- DropBox
- DropBox for Business (apenas para Windows)

  NOTA:
  Dependendo da versão do Dell Server utilizada pela sua empresa, é possível encriptar todos os ficheiros e pastas nas contas pessoais Dropbox que estão ligados a contas da empresa.
- Box

  NOTA:
  O Box Tools e o Box Edit não são suportados pelo Data Guardian. Utilizar o Box Tools pode provocar uma condição de ecrã azul.
- Google Drive

  NOTA:
  A cópia de segurança e a sincronização da Google não são suportadas.
- OneDrive
- OneDrive for Business
- Unified OneDrive

  NOTA:
  O Unified OneDrive consiste num cliente de sincronização unificado para o OneDrive e para o OneDrive para Empresas.

Microsoft Office

O Data Guardian suporta as seguintes versões do Office. No entanto, é preciso ter apenas uma versão do Office instalada.

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus: 1705 diferida, 1708 semestral e 1803 mensal

Data Guardian para Mac

Segue-se uma lista do hardware suportado para o cliente Mac.

Hardware para Mac

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

Sistemas operativos

Segue-se uma lista dos sistemas operativos suportados.

Sistemas operativos para Mac

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

Fornecedores de armazenamento na nuvem

Com base nas definições das políticas, pode ser apresentado o seguinte na interface do Data Guardian para Mac. O utilizador não precisa de transferir ou instalar o cliente de sincronização na nuvem.

Fornecedores de armazenamento na nuvem

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

Aplicação móvel do Data Guardian

Segue-se uma lista dos sistemas operativos suportados pela aplicação móvel Data Guardian.

Sistemas operativos para 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 operativos 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 que instala o cliente Web e comunica com a versão v9.8 ou posterior do Dell Server.

Os seguintes ambientes virtuais podem ser utilizados para implementar o cliente Web do Data Guardian.

Ambientes virtuais

- VMware ESXi 6.0
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-60/index.jsp para obter mais informações
- VMware ESXi 5.5
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo

Ambientes virtuais

- Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
- O hardware deve cumprir os requisitos mínimos do VMware
- RAM mínima de 4 GB para recurso de imagem dedicado
- Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações

Web browsers

Pode utilizar o Data Guardian com o Internet Explorer, Mozilla Firefox, Google Chrome e Microsoft Edge.

Para Mac; também é suportado o Safari.

Suporte de idiomas

Estes clientes seguem a norma MUI (Interface de Utilizador Multilingue) e suportam os seguintes idiomas.

Suporte de idiomas

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

Configurar e instalar o Data Guardian no Windows

Definições do registo do cliente Data Guardian

Esta secção explica todas as definições de registo aprovadas pelo Dell ProSupport para computadores cliente locais, independentemente do motivo da definição de registo. Se uma configuração de registo se sobrepõe a dois produtos, está indicada em cada uma das categorias.

Estas alterações de registo apenas devem ser efetuadas por administradores e poderão não ser adequadas ou funcionar em todos os cenários.

- Os níveis de registo podem ser aumentados para ajudar na resolução de problemas. Crie ou modifique a seguinte definição de registo.

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

  "LogVerbosity"=dword:0x1f (31)

  Por predefinição, o nível de registo está definido para 0xf (15).

  Valores disponíveis:

  Desativado=0x0 (0)

  Crítico=0x1 (1)

  Erro=0x3 (3)

  Aviso=0x7 (7)

  Informação=0xf (15)

  Depuração=0x1f (31)

- Após a instalação do Data Guardian, os utilizadores internos são automaticamente ativados. Se necessário, pode modificar a definição do registo para ignorar a ativação automática.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valor DWORD: DisableAutomaticActivation=1

NOTA:
Também pode confirmar os aliases para o seu domínio no Dell Server. Consulte Resolução de problemas de ativação automática.

Configurar o servidor para o Data Guardian

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

- Documentos do Office armazenados localmente, partilhados com outros utilizadores de várias formas, ou guardados em suportes de dados amovíveis. Podem ser protegidos os seguintes tipos de documentos do Office: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- Sistemas de partilha de ficheiros baseados na nuvem - dispositivos móveis ou computadores Windows captam os dados destinados ao armazenamento na nuvem, encriptam esses dados e, em seguida, carregam os dados encriptados para a nuvem.

Informe os utilizadores se a sua empresa só utilizar o Data Guardian com documentos do Office, apenas no armazenamento em nuvem ou em ambos.

Configurar o Dell Security Management Server Virtual para o Data Guardian

Para configurar o Dell Security Management Server Virtual para suportar o Data Guardian, na Management Console, defina uma ou ambas as políticas do Data Guardian como **Ligadas**:

- *Documentos do Office protegidos* - apenas nível Enterprise
- *Encriptação da nuvem* - nível Enterprise, Endpoint Groups ou Endpoints

Configurar o Security Management Server para o Data Guardian

Para configurar o Dell Security Management Server para suportar o Data Guardian, na Management Console, defina uma ou ambas as políticas do Data Guardian como **Ligadas**:

- *Documentos do Office protegidos* - apenas nível Enterprise
- *Encriptação da nuvem* - nível Enterprise, Endpoint Groups ou Endpoints

Em seguida, configure o Security Server para permitir transferências do cliente da nuvem.

Configurar o Security Management Server para permitir transferências do Data Guardian

Esta secção descreve os passos necessários para permitir aos utilizadores transferir o cliente Data Guardian para Windows a partir do seu Security Management Server.

1. No Security Management Server, aceda a *<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources* e abra o ficheiro *messages.properties* com um editor de texto.
2. Certifique-se de que as entradas são as seguintes:

   download.deviceWin.mode=remote

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

   download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe
3. Editar as entradas para o seguinte

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

   download.deviceWin.remote.link.64=https://<O URL DO SEU ANFITRIÃO>:<PORTA>/cloudweb/download/DataGuardian_64bit_setup.exe
4. Guarde e feche o ficheiro.
5. Aceda a <Security Server install dir> e crie uma nova pasta chamada Download (Security Server\Download).
6. Na pasta Transferências, crie outra pasta chamada cloudweb (Security Server\Transferências\cloudweb).
7. Adicione os ficheiros de configuração de 64 bits e 32 bits do Data Guardian à pasta cloudweb, podendo mudar os nomes para, por exemplo, DataGuardian64.exe e DataGuardian32.exe, respetivamente.

   Estes são definidos pelo utilizador, mas têm de coincidir com os nomes dos ficheiros no ficheiro versions.xml.
8. Reinicie o Security Server para que as alterações surtam efeito.

Configurar o Security Management Server para transferência automática do cliente Data Guardian do Windows (opcional)

Para transferências automáticas, o ficheiro versions.xml e os binários devem encontrar-se na mesma localização. O cliente deve poder aceder à localização, por isso pode ser IIS ou pode utilizar a pasta **Security Server\Transferências\cloudweb** que criou. Se estiver a utilizar a pasta cloudweb, siga este exemplo de configuração.

1 Aceda à pasta **Security Server\Transferências\cloudweb**. (Consulte o passo 6 em Configurar o Security Server para permitir transferências do cliente Data Guardian.)

2 Crie uma pasta secundária com o nome DataGuardianUpdate.

NOTA:
O nome DataGuardianUpdate é utilizado neste exemplo, mas pode escolher qualquer nome.

3 Coloque os ficheiros executáveis atualizados na pasta DataGuardianUpdate.

4 Crie um ficheiro *version.xml* na pasta DataGuardianUpdate.

5 Abra *versions.xml* com um editor de texto e certifique-se de que o caminho do nome do ficheiro é 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 do ficheiro dos executáveis atualizados

Nome de ficheiro setup.exe: o nome de configuração dos ficheiros executáveis é definido pelo utilizador mas deve corresponder ao nome de configuração do ficheiro messages.properties. (Consulte o passo 3 em Configurar o Security Server para permitir transferências do cliente Data Guardian.)

6 Guarde e feche o ficheiro.

7 Adicione os binários a esta pasta.

8 Se estiver a utilizar o IIS, reinicie o IIS.

9 Como administrador Dell, inicie sessão na Management Console.

10 No painel esquerdo, clique em **Populações** > **Empresa** e é apresentado o separador Políticas de segurança.

11 No grupo de tecnologia Data Guardian, clique em **Encriptação na nuvem** > **Mostrar definições avançadas**.

12 Desça até à política de *URL de Servidor de atualização do software* e introduza **https://<O URL DE ANFITRIÃO> > / DataGuardianUpdate**.

NOTA:
O nome DataGuardianUpdate é apenas um exemplo para corresponder ao exemplo anterior.

13 Clique em **Guardar** para armazenar a alteração à política na fila para consolidar.

14 Clique em **Gestão** > **Consolidar**.

15 Introduza um comentário e clique em **Consolidar políticas**.

Recriar imagem de um computador com Data Guardian instalado

Se for necessário recriar a imagem do computador e este tiver o Data Guardian instalado, pergunte ao utilizador se trabalhou offline e criou algum documento do Office protegido enquanto estava offline. Se for esse o caso, foram geradas chaves offline para esses documentos e essas chaves não foram caucionadas para o Dell Server.

1 Para obter informações sobre a recuperação de chaves do Data Guardian geradas offline que não foram caucionadas para o Dell Server, consulte o *Guia de recuperação*.

2 Verifique se há uma pasta de chaves offline antes de recriar a imagem do computador.

Quando são criadas as primeiras chaves de caução, é adicionada uma pasta Data Guardian em C:\Program Files\Dell. Aceda à pasta Data Guardian > OfflineKeys. Se a pasta OfflineKeys não existir, consulte a pasta Os meus documentos do utilizador.

Desativar o Exploit Guard da Microsoft ou o EMET para Aplicações geridas

No Windows 10, os seguintes itens podem estar ativados ou integrados no SO:

- Redstone 3 ou posterior – Windows Defender Exploit Guard (WDEG)
- Redstone 2 ou anterior – Enhanced Mitigation Experience Toolkit (EMET)

Se estas funcionalidades estiverem ativadas ou integradas, tem de configurar as definições para desativar estas aplicações geridas para o Data Guardian:

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

Windows Defender Exploit Guard (WDEG)

Para desativar as aplicações geridas:

1 Aceda ao **Centro de Segurança do Windows Defender**.
2 Clique em **Controlo de aplicações e browsers**.
3 Navegue para o final da página e clique em **Definições de proteção do Exploit**.
4 Selecione **Definições de programas**.
5 Clique em **+** para adicionar cada aplicação gerida listada acima.
6 Nas Propriedades de cada aplicação gerida, selecione a caixa de verificação *Ignorar* para todas as opções definidas para *Ligada* e defina a opção para **Desligada**.

> **NOTA:**
> Se uma aplicação gerida estiver aberta e uma caixa de diálogo indica que tem de reiniciar o ficheiro .exe, reinicie-o após concluir estes passos.

7 Clique em **Aplicar**.
8 Clique em **Sim**.

Nas Definições de programas, a aplicação gerida lista as substituições com base nas opções que alterou.

Enhanced Mitigation Experience Toolkit (EMET)

Para desativar as aplicações geridas:

1 Aceda à **Configuração da aplicação**.
2 Nas opções **Verificação de chamador ROP** e **Exportar filtro de acesso à tabela de endereços (EAF)**, desmarque as caixas de verificação das aplicações geridas listadas acima.

Gerir perfis de fornecedor de proteção de armazenamento na nuvem

O Data Guardian encripta os ficheiros dos utilizadores e envia eventos de auditoria para o Dell Server. Para alterar o comportamento de cada fornecedor de armazenamento na nuvem suportado, defina cada fornecedor para um destes valores:

Valor	Descrição
Proteger	Permitir o fornecedor/ligação, encriptar os ficheiros e enviar eventos de auditoria sobre a atividade do ficheiro/pasta.
Bloquear	Bloqueie todo o acesso ao fornecedor/ligação.
Permitir	Permitir o fornecedor/ligação a passar sem encriptação, mas efetuar uma auditoria à atividade do ficheiro/pasta.
Ignorar	Ignorar a proteção do fornecedor/ligação sem encriptar ou efetuar auditoria. Quando este valor é definido, a pasta do fornecedor de armazenamento em nuvem não é apresentada na unidade virtual do Data Guardian no computador cliente.

Para obter mais informações, consulte *AdminHelp*, que está acessível a partir da Remote Management Console do Dell Server.

Permitir/recusar utilizadores na Lista de acesso completo/lista negra

Pode determinar os utilizadores externos que se podem registar com o Dell Server para utilizar o Dell Server. Para uma segurança adequada, certifique-se de que configura e gere cuidadosamente estas listas.

- Um utilizador interno está dentro do domínio.
- Um utilizador externo é um utilizador exterior ao domínio; poderá tratar-se de uma pessoa de outra organização com a qual um utilizador interno pretende partilhar documentos confidenciais da empresa ou um utilizador interno que pretende aceder ao respetivo computador a partir de um dispositivo externo ao dispositivo.

Para permitir a um utilizador que não esteja incluído no domínio da organização registar-se para utilizar o Data Guardian:

1 No painel esquerdo da Remote Management Console, clique em **Gestão > Gestão de utilizadores externos**.

2 Clique em **Adicionar**.

3 Selecione Tipo de acesso ao registo:

Lista negra - bloqueia o registo de um utilizador ou domínio. O utilizador não pode abrir um documento do Office protegido ou ficheiro .xen.

Lista de acesso total - concede acesso ao registo e a todos os ficheiros para um utilizador ou domínio. Se um utilizador ou domínio também estiverem na lista negra, não é concedido qualquer acesso.

4 No campo Introduzir domínio/e-mail, introduza o domínio do utilizador para definir o acesso a todo o domínio ou o endereço de e-mail para definir o acesso apenas a esse utilizador.

NOTA: Para utilizadores móveis externos num ambiente alojado, o e-mail tem de estar em minúsculas.

5 Clique em **Adicionar**.

Para obter mais informações sobre como utilizar a lista de acesso total/lista negra, consulte *AdminHelp*, acessível a partir de Management Console.

Instalar o Data Guardian

Existem dois métodos para instalar o Data Guardian:

- Instalar o Data Guardian interactivamente
- Instalar o Data Guardian com a Linha de comandos

Os utilizadores do Data Guardian têm de realizar as seguintes tarefas para protegerem os ficheiros e pastas dos respetivos clientes de sincronização na nuvem. Após a instalação do cliente Data Guardian, os utilizadores devem transferir um fornecedor de armazenamento na nuvem:

- O administrador deve especificar o fornecedor de armazenamento na nuvem a utilizar.

  ou

- Forneça aos utilizadores uma ligação para transferência e instalação do Dropbox for Business ou OneDrive para Empresas/Unified OneDrive, se a sua empresa utilizar um destes fornecedores. Lembre-se de que os utilizadores do Dropbox for Business devem ligar-se ao Dropbox for Business através do Data Guardian.

Pastas preexistentes com ficheiros não encriptados

Ao implementar o Data Guardian, é preferível que os dispositivos de destino não tenham ainda as contas configuradas as contas do fornecedor de armazenamento na nuvem.

Se um fornecedor de armazenamento na nuvem estiver configurado com pastas sincronizadas com o computador local antes da instalação do Data Guardian:

- Os ficheiros e pastas preexistentes que são sincronizados para a nuvem permanecem em texto desencriptado
- Os ficheiros que adicionar a essas pastas preexistentes permanecem em texto desencriptado
- Os ficheiros que são sincronizados a partir da nuvem são encriptados

  Se pretender que os ficheiros pré-existentes sejam encriptados, aceda à Unidade virtual DDG VDisk (criada durante a instalação do Data Guardian), crie uma nova subpasta dentro do cliente de sincronização na nuvem e mova os ficheiros pré-existentes para essa pasta.

  ou

  Para conteúdos de grande dimensão, um gestor ou administrador pode solicitar temporariamente o Menu Gerir pastas.

Menu Gerir pastas

Alguns gestores ou administradores podem ter de efetuar temporariamente a solução de problemas de pastas partilhadas por mais do que um utilizador. Pode solicitar permissão ao seu administrador para a opção Gerir pastas. Normalmente, esta é uma opção temporária.

Instalar o Data Guardian interativamente no Windows

Apenas um administrador local tem permissão para instalar o Data Guardian. Se forem os utilizadores a instalar o produto, informe-os sobre a localização do suporte de instalação.

Antes de começar

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

Dell Security Center alojado	No local (para Dell Management Server	Encriptação em nuvem
Para lançamento futuro.	Certifique-se de que sabe o nome do Dell Security Management Server.	O computador deve ter uma letra do alfabeto disponível para atribuir a uma unidade de disco.

Instalar o Data Guardian

Esteja preparado para reiniciar o computador após a instalação do Data Guardian.

1 Para transferir o instalador do Data Guardian, aceda à localização especificada pelo seu administrador.

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

3 Clique duas vezes no ficheiro para iniciar o programa de instalação.

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

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

6 Caso apareça uma mensagem a questionar se deseja instalar o Pacote redistribuível do Microsoft Visual C++ 2015 ou o Microsoft .NET Framework 4.5.2 Client Profile, clique em **OK**.

7 No ecrã de boas-vindas, clique em **Seguinte**.

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

9 No ecrã Pasta de destino, clique em **Seguinte** para instalar na localização predefinida de **C:\Program Files\Dell\Data Guardian\.**

Em **C:**, não instale o Data Guardian nas pastas Utilizadores ou Windows, nem na raiz de qualquer unidade. Nesse caso, é obtido um erro.

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

Dell Security Center alojado	Dell Management Server no local
Para lançamento futuro.	No campo `Dell Management Server Name:`, introduza o nome do servidor com o qual este computador vai comunicar, como, por exemplo, servidor.domínio.com. Não é necessário incluir web ou http(s). Esta informação é fornecida pelo seu administrador. Não desmarque a caixa de verificação *Ativar verificação de confiança SSL* exceto se tal for instruído pelo administrador.

11 Clique em **Seguinte**.

12 No ecrã Confirmar informações do Dell Management Server, certifique-se de que o endereço URL do servidor está correto. O instalador adiciona www ou http(s) e, de seguida, a porta. Clique em **Seguinte**.

13 Na janela Tipo de gestão, selecione esta opção:

- Uso interno - Um utilizador com um endereço de e-mail dentro do domínio da empresa.

14 Clique em **Instalar** para dar início à instalação.

Uma janela de estado apresenta o progresso da instalação.

15 Clique em **Concluir** quando for apresentado o ecrã de Instalação concluída.

16 Clique em **Sim** para reiniciar.

A instalação do Data Guardian está concluída.

17 Instrua os utilizadores finais para confirmarem a ativação. O ícone do tabuleiro do sistema do Data Guardian deverá ter uma marca de verificação verde  . Dependendo da forma como o Data Guardian é implementado dentro da empresa, a ativação pode não ser imediata. Caso contrário, o utilizador final deve efetuar a ativação manualmente. Num ambiente alojado, um utilizador que ative manualmente tem de reativar sempre que reinicia o computador ou o serviço Data Guardian. Consulte o *Data Guardian User Guide* (Guia do utilizador do Data Guardian).

Instalar o Data Guardian com a Linha de comandos

- As opções e parâmetros da linha de comandos são sensíveis a maiúsculas e minúsculas.
- Certifique-se de que inclui um valor que contenha um ou mais caracteres especiais, como um espaço em branco na linha de comandos, entre aspas duplas de escape.
- A tabela seguinte descreve as opções disponíveis para a instalação.

Opção	Significado
/V	Passa variáveis para o .msi dentro do setup.exe. O conteúdo deve estar sempre dentro de aspas de texto simples.
/S	Modo silencioso

Opção	Significado
/QB	Caixa de diálogo de Progresso com botão **Cancelar**, solicita o reinício
/QB!	Caixa de diálogo de Progresso sem botão **Cancelar**, solicita o reinício
/QN	Sem interface de utilizador

- A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
SERVER=<NomedoServidor> (FQDN do Servidor Dell para ativação)
ENTERPRISE=1 (Utilizador interno)
ENABLESSLTRUST=0 (Desativar validação fidedigna SSL)
REBOOT=SUPPRESS (o zero permite a reinicialização automática, SUPPRESS desativa a reinicialização)

Exemplo de linha de comandos

- O exemplo seguinte instala o Data Guardian silenciosamente, para um utilizador interno, sem validação fidedigna SSL; os registos são armazenados em C:\Biblioteca\Registos\Install.log.

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

Definir GPO no controlador do domínio para ativar as elegibilidades

- Se os clientes forem elegíveis partir do Dell Digital Delivery, siga estas instruções para definir o GPO no controlador de domínio e ativar as elegibilidades (não deve ser o mesmo servidor que está a executar o Dell Server).
- A estação de trabalho deve fazer parte da UO onde o GPO está aplicado.
- Certifique-se de que a porta de saída 443 está disponível para comunicar com o Dell Server. Se a porta 443 estiver bloqueada (por qualquer motivo) a funcionalidade de elegibilidade não funciona.

1. No controlador de domínio para gerir os clientes, clique em **Iniciar** > **Ferramentas administrativas** > **Gestão de Políticas de Grupo**.
2. Clique com o botão direito do rato na OU onde a política deve ser aplicada e selecione **Criar um GPO neste domínio** e **Ligá-lo aqui**.
3. Introduza um nome para o novo GPO, selecione (nenhum) para GPO de arranque de origem e clique em **OK**.
4. Clique com o botão direito no GPO que foi criado e selecione **Editar**.
5. É carregado o Editor de gestão de política de grupo. Aceda a **Configuração do computador** > **Preferências** > **Definições do Windows** > **Registo**.
6. Clique com o botão direito do rato no Registo e selecione **Novo** > **Item do registo**. Execute as seguintes ações.

   Ação: Criar

   Ramo de registo: HKEY_LOCAL_MACHINE

Caminho da chave: SOFTWARE\Dell\Dell Data Protection

Nome do valor: Servidor

Tipo do valor: REG_SZ

Dados do valor: <Endereço IP do Dell Server>

7 Clique em **OK**.

8 Termine sessão e, em seguida, inicie novamente sessão na estação de trabalho ou execute **gpupdate /force** para aplicar a política de grupo.

Desinstalar o Data Guardian

- Se um **utilizador final** tiver uma conta de administrador local, pode desinstalar o Data Guardian. Consulte o *Guia de utilizador do Data Guardian* para obter informações. Esta secção descreve o processo de administrador de desinstalação do Data Guardian.

> **IMPORTANTE: ficheiros não Office na Unidade virtual DDG VDisk**
> Antes de desinstalar o Data Guardian, mova todos os ficheiros importantes para uma localização fora da Unidade virtual DDG VDisk. Quando o Data Guardian é desinstalado a partir de um computador de utilizador final, as suas pastas e ficheiros na nuvem estarão encriptados e serão ilegíveis. Se este utilizador final abandonar a empresa e nenhum outro utilizador partilhar essa pasta ou ficheiro, os dados são ilegíveis mas seguros (para visualizar os ficheiros, poderia reinstalar o Data Guardian).
>
> Os documentos do Office protegidos permanecem encriptados se desinstalar o Data Guardian. Para desencriptar, consulte o *Guia de recuperação > Recuperação do Data Guardian*.

Desinstalação por linha de comando

- Uma vez extraído do instalador principal, o instalador do cliente do Data Guardian pode ser localizado em **C:\Dell \DataGuardian_XXbit_setup.exe**.
- O seguinte exemplo desinstala o cliente do Data Guardian de forma silenciosa.

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

Reinicie o computador quando solicitado.

Utilizar o Data Guardian com o Dropbox for Business

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

É possível definir políticas para controlar a proteção das pastas empresariais e pessoais no Dropbox. Se a sua empresa permitir contas empresariais e pessoais, os utilizadores finais devem compreender a encriptação de cada tipo de conta. Consulte Política para contas empresariais e pessoais.

Política para contas empresariais e pessoais

A sua empresa pode ter diretrizes que definem se os membros da equipa podem utilizar contas empresariais e pessoais. Além disso, a empresa poderá permitir que apenas determinados utilizadores tenham contas empresariais e pessoais.

> **NOTA:**
> Se a sua empresas permitir contas empresariais e pessoais, e um utilizador final optar por utilizar ambas, o utilizador deve compreender a gestão das pastas de ambos os tipos de contas.

A tabela seguinte descreve a encriptação com base na definição da política *Pastas pessoais encriptadas do Dropbox*.

Encriptação	Definição de política	Considerações sobre a implementação
Encripte todos os ficheiros e pastas empresariais e pessoais.	Política > Pastas pessoais encriptadas do Dropbox > definido como **Selecionado** (predefinição)	Antes de o Data Guardian ser implementado, os utilizadores devem fazer uma cópia de segurança dos ficheiros empresariais previamente existentes que estão em pastas de sincronização com o armazenamento na nuvem para localizações fora das pastas de sincronização. Os utilizadores com ficheiros pessoais que deverão permanecer desencriptados terão de mover os ficheiros para fora das pastas de sincronização empresariais ou desagregar as contas pessoais dos cliente de sincronização empresariais. Quando o Data Guardian estiver implementado, os ficheiros e pastas na nuvem podem ser visíveis apenas em computadores ou dispositivos que executem o Data Guardian. Se uma pasta pessoal for encriptada inadvertidamente, consulte "Desencriptar pastas numa conta pessoal" no Guia do Utilizador do Dell Data Guardian.
Encripte todos os ficheiros e pastas de contas empresariais. Permita que ficheiros e pastas de contas pessoais permaneçam não encriptados.	Política > Pastas pessoais encriptadas do Dropbox > definido como **Não selecionado**	Pode utilizar a política opcional de Mensagem de pastas pessoais encriptadas do Dropbox para visualizar uma mensagem personalizada para lembrar os utilizadores para **não** armazenarem ficheiros empresariais em contas pessoais, uma vez que esses ficheiros não serão protegidos. A mensagem é apresentada neste momento: • Sempre que o utilizador iniciar sessão • Quando o utilizador criar ou adicionar um novo ficheiro ou pasta a uma conta pessoal do Dropbox Se definir a política Pastas pessoais encriptadas do Dropbox para **Falso** para um Endpoint ou Grupo de endpoints, as contas pessoais de todos os utilizadores nesses endpoints irão permanecer desencriptadas.

Pastas empresariais e pessoais

Se a sua empresa tiver o Dropbox for Business e permitir que os utilizadores finais possuam pastas empresarias e pessoais, poderá pretender realizar relatórios que garantam que todos os ficheiros empresariais têm a extensão de ficheiro .xen, caso um utilizador final copie um ficheiro não protegido sensível para uma pasta empresarial. Consulte Resolução de problemas do Data Guardian.

Ver relatórios

Estão disponíveis informações sobre o seu ambiente Data Guardian na Management Console. Selecione **Relatórios > Eventos de auditoria** para eventos de auditoria relacionados com a sincronização de pastas de cliente na nuvem e documentos do Office protegidos.

Para efeitos de conformidade e monitorização dos detalhes do dispositivo, detalhes Shield ou eventos de auditoria, consulte **Relatórios > Gerir relatórios**.

Para obter mais informações, consulte *AdminHelp*, que está acessível a partir da Management Console.

Resolução de problemas do Data Guardian

Utilize o Ecrã Detalhes

Pode utilizar o ecrã *Detalhes* para a resolução de problemas ou problemas de suporte. Por exemplo:

- Se um utilizador criar uma pasta, mas não estiver a encriptar, selecione **Detalhes** > **Ficheiros** > **Estado da pasta** para verificar o estado.
- Se um utilizador final solicitar suporte, é possível fornecer-lhe instruções para configurar o ecrã Detalhes Melhorados e selecionar o separador **Detalhes** > **Política**. Este separador apresenta as políticas implementadas.
- Consulte os registos para a resolução de problemas.

Utilizar o Ecrã Detalhes Melhorados

- Enquanto prime **<Ctrl><Shift>**, clique no ícone do tabuleiro do sistema do Data Guardian e, em seguida, selecione **Detalhes**.
- Para além de Ficheiros e Pastas, é apresentado o seguinte:

  Segurança: indica a chave, tipo de chave e estado. Este painel indica temporariamente alguns ficheiros do Office protegidos até que sejam enviados para o Dell Server; o período de tempo depende do intervalo de consulta.

  Auditoria: indica módulos, ID de utilizador e tipo de evento. As informações estão em fila neste registo de auditoria e, em seguida, são enviadas para o Dell Server em intervalos especificados. O administrador pode visualizar **Eventos de auditoria** no painel esquerdo da Management Console para auditoria.

  Política: indica os valores e nomes das políticas.

Visualizar ficheiros de registo

- Clique em **Ver Registo** no canto inferior esquerdo do ecrã Detalhes.

  Os ficheiros de registo também estão disponíveis em **C:\ProgramData\Dell\Data Guardian**.

  Os ficheiros de registo dos documentos do Office protegidos encontram-se na Custom.xml.

Resolução de problemas de ativação automática

Se o Data Guardian não se ativar automaticamente para vários utilizadores, é possível alterar as Definições do registo do cliente Data Guardian. Também deve verificar os aliases no Dell Server:

1. Na Management Console, navegue até **Populações > Domínios** e selecione um domínio e quaisquer subdomínios.
2. Na página Detalhe do domínio, clique no separador **Definições**.
3. No campo *Alias*, confirme que todos os alias estão corretos.

Atribuir direitos temporários de gestão de pastas

Pode conceder a um administrador ou utilizador direitos temporários para gerir pastas. Por exemplo, se os utilizadores tiverem carregado ficheiros para a nuvem antes da instalação do Data Guardian, pode atribuir direitos temporários de Gestão de pastas a alguns utilizadores, para gerir a encriptação pasta a pasta, dentro das pastas do cliente de sincronização.

Para atribuir direitos de gestão de pastas:

1 Na Management Console, clique em **Populações** > **Endpoints**.

2 Procure ou clique num ponto final e, em seguida, clique no separador **Políticas de segurança**.

3 Selecione **Encriptação na nuvem** e, em seguida, clique em **Mostrar definições avançadas.**

4 Clique na caixa de verificação junto a *Gestão de pastas ativada* para selecionar a política.

5 Clique em **Guardar**.

6 No painel da esquerda, clique em **Gestão** > **Consolidar**.

7 Introduza um comentário e clique em **Consolidar políticas**.

NOTA:
A Dell recomenda que, depois de as pastas estarem encriptadas ou resolução de problemas estar concluída, desmarque a caixa de verificação da política *Gestão de pastas ativada* para desativar a política para esse ponto final.

Para gerir pastas no ponto final:

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

2 Clique no ícone do tabuleiro do sistema do Data Guardian e selecione **Gerir pastas**.

Uma vista hierárquica das pastas sincronizadas na nuvem é exibida para cada cliente de sincronização. Todas as pastas estão selecionadas por predefinição. Anule a seleção das pastas que não pretende encriptar. Se anular a seleção de uma pasta em Gerir pastas, é realizada uma ação de desencriptação dos ficheiros existentes nessa pasta. Não são encriptados ficheiros novos nessa pasta, na unidade local ou na nuvem.

NOTA:
Se arrastar um ficheiro encriptado para dentro de uma pasta que não está selecionada em Gerir pastas, na nuvem ou na unidade virtual do Data Guardian, o ficheiro permanece encriptado e não é possível ver o conteúdo. Além disso, se partilhar a pasta com outro utilizador do Data Guardian que não tenha ativada a política Gerir pastas, os ficheiros permanecem encriptados e não é possível ver o conteúdo.

3 Para encriptar uma pasta pré-existente, ative manualmente a encriptação para essa pasta. Os ficheiros são encriptados depois de serem sincronizados para a nuvem.

Perguntas frequentes

Perguntas frequentas sobre a gestão de pastas

Pergunta

Tenho uma pasta com ficheiros que partilhei com outro utilizador. No tabuleiro do sistema, utilizei o utilitário **Data Guardian > Gerir pastas** para desencriptar os conteúdos dessa pasta. Recentemente, os meus ficheiros ficaram novamente encriptados na nuvem. A pasta em questão já não é apresentada no utilitário Gerir pastas; por conseguinte, já não posso desencriptar estes ficheiros na nuvem.

Resposta

Uma ID da chave de encriptação é associada a uma pasta com base no primeiro utilizador que adiciona um ficheiro à mesma. Se um utilizador criar uma pasta e não adicionar quaisquer ficheiros, a chave não é associada a essa pasta. O utilizador cuja ID da chave de encriptação foi definida na pasta é o único que pode ver a pasta no utilitário Gerir pastas. Se o utilizador cuja ID de chave de encriptação está definida na pasta anular a seleção da pasta no utilitário Gerir pastas e partilhar essa pasta com outro utilizador do Data Guardian, o Data Guardian do segundo utilizador volta a encriptar o conteúdo.

Solução

1 Crie uma nova pasta.

2 Mova todos os ficheiros que pretende encriptar para a nova pasta.

3 No tabuleiro do sistema, utilize novamente o utilitário **Dell Data Guardian** > **Gerir pastas** para desencriptar esses ficheiros.

NOTA:

Se desencriptar o conteúdo de uma pasta partilhada com outro utilizador do Data Guardian, o cliente Data Guardian do outro utilizador irá aplicar a política para os encriptar. A prática recomendada é utilizar o utilitário Gerir pastas para desencriptar apenas os ficheiros que não são partilhados com outros utilizadores do Data Guardian.

Pergunta

Estou a sincronizar uma pasta desencriptada que desmarquei com o utilitário Gerir pastas. No entanto, quando tento carregá-la através do Web browser, apenas consigo carregar ficheiros encriptados.

Resposta

O Data Guardian não foi concebido para pesquisar ativamente pastas na nuvem. Com pastas não encriptadas, o Data Guardian pode sincronizar através do cliente de sincronização porque este controla o ambiente. Os ficheiros que passam pelo Web browser devem ser encriptados.

Solução

Adicione ficheiros à pasta de sincronização.

Pergunta

Recentemente, desinstalei do meu computador o meu sistema de partilha de ficheiros baseado na nuvem, mas quando abri o utilitário Gerir pastas, um dos clientes de sincronização continuava a aparecer como opção.

Resposta

O Data Guardian não monitoriza a instalação nem a desinstalação de softwares provenientes de terceiros. Estas opções continuam a ser apresentadas, porque, de acordo com a respetiva conceção, quando esses clientes são desinstalados, não removem os ficheiros existentes. Esses ficheiros continuam a ser protegidos pelo Data Guardian, embora o cliente de sincronização não se encontre mais instalado.

Solução

Para remover a opção de cliente de sincronização desinstalada do utilitário Gerir pastas, mova quaisquer pastas/ficheiros que pretende manter para fora da pasta de sincronização e, em seguida, elimine a pasta. Após a eliminação da pasta, esta deixa de ser apresentada no utilitário Gestão de pastas.

Perguntas frequentes variadas

Pergunta

Um utilizador possui Data Guardian com Documentos do Office protegidos e não consegue copiar nem colar.

Resposta

No Data Guardian, algumas funcionalidades são processadas pelo tabuleiro do sistema. Verifique se o utilizador modificou o tabuleiro do sistema.

Solução

Devem ser utilizadas as predefinições do tabuleiro do sistema. O utilizador deverá manter as predefinições do tabuleiro do sistema.

Pergunta

Alterei a política **Ocultar nomes de ficheiros** de Guid para Apenas extensão. No entanto, as pastas que estava anteriormente a sincronizar continuam a encriptar estes ficheiros para o outro formato com nomes de ficheiros Guid. Por quê?

Resposta

Quando é alterada uma política no Security Management Server/Security Management Server Virtual, o Data Guardian mantém a política anterior para essa pasta. A nova política será aplicada às novas pastas criadas, sendo encriptadas com o formato **Apenas extensão**.

Solução

Para aplicar novamente o formato **Apenas extensão** aos ficheiros antigos, corte e cole os ficheiros numa nova pasta onde seja aplicada a nova política.

Configurar e instalar o Data Guardian no Mac

O Data Guardian para Mac foi concebido para partilhar ficheiros dentro de fornecedor de encriptação de nuvem. No entanto, se as políticas de Documentos do Office protegidos estiverem ativadas para Mac, perde-se a auditoria e o rastreio de todos os ficheiros se estes forem guardados pelo utilizador no Mac local. Se a sua organização necessitar de auditoria e de rastreio rigorosos, defina a política *Permitir ativação Mac do Data Guardian* como **Não selecionado** para impedir que o Data Guardian seja ativado em computadores Mac.

Tarefas do servidor

Pré-requisitos

Antes de executar estas tarefas, confirme o seguinte:

- Instale o Dell Server e os respetivos componentes. Consulte uma das seguintes opções:
  - *Guia de instalação e migração do Security Management Server*
  - *Guia de instalação e Guia de início rápido do Security Management Server Virtual*
- Na Management Console, atribua a função de administrador Dell adequada.

Políticas

Por predefinição, o Data Guardian encripta os ficheiros dos utilizadores e envia eventos de auditoria para o Security Management Server Virtual. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Security Management Server Virtual).

Se pretender que os eventos de auditoria incluam dados de geolocalização, deve ativar a rede Wi-Fi. Para obter mais informações sobre a geolocalização e eventos de auditoria, consulte *AdminHelp*.

Para alterar o comportamento predefinido para cada fornecedor de armazenamento em nuvem suportado, defina a política *Fornecedor de proteção de armazenamento em nuvem*. Se a sua empresa prefere um fornecedor de armazenamento em nuvem específico, defina esta política como **Bloquear** para outros fornecedores. Para obter mais informações acerca das políticas, consulte *AdminHelp*, que está acessível a partir da Management Console.

NOTA:
A opção Ignorar desta política destina-se ao Windows. Se selecionar Ignorar para Mac, será apresentada ao utilizador final como Permitir.

Configurar o Security Server para autorizar transferências de clientes na nuvem

Antes de executar estas tarefas, confirme o seguinte:

- Instale o Dell Server e os respetivos componentes. Consulte uma das seguintes opções:
  - *Guia de instalação e migração do Security Management Server*
  - *Guia de instalação e Guia de início rápido do Security Management Server Virtual*
- Na Management Console, atribua a função de administrador Dell adequada.

Security Management Server

1 No Security Management Server, aceda a <Security Server install dir>\webapps\cloudweb\brand\dell\resources\
2 Abra o ficheiro **messages.properties** com um editor de texto.
3 Certifique-se de que 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://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

4 Guarde e feche os ficheiros.
5 Aceda a <Security Server install dir> e crie uma pasta chamada Transferências (Security Server\Transferências).
6 Na pasta Download, crie uma pasta CloudWeb (Security Server\Download\CloudWeb).
7 Adicione os programas de instalação do Dell Data Guardian a essa pasta.

Virtual Edition: instalar manualmente uma versão diferente do cliente de nuvem

Não é necessária qualquer ação para permitir que os utilizadores transfiram o programa de instalação do cliente Dell Data Guardian mais recente. O instalador mais recente está pré-instalado no Security Management Server Virtual Security Server.

Para instalar manualmente uma versão diferente do instalador do Data Guardian no Security Management Server Virtual Security Server, atualize o ficheiro message.properties.

1 Aceda a:
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Abra o ficheiro **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://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
```

3 Guarde e feche os ficheiros.

4 Copie os ficheiros para /opt/dell/server/security-server/transferências/cloudweb.

5 Adicione os programas de instalação do Data Guardian a essa pasta.

Permitir/recusar utilizadores na Lista de acesso completo/lista negra

As entradas na de acesso total e na lista negra determinam que utilizadores podem registar-se no Dell Server para utilizar o Data Guardian.

Lista de acesso total

A lista de acesso total permite que utilizadores ou grupos de utilizadores específicos se registem no Dell Server e utilizem o Data Guardian.

Os utilizadores externos devem ser colocados na lista de acesso total para permitir o registo. Consulte os exemplos seguintes para permitir que os utilizadores se registem:

Tipo de utilizador	Introduzir
Todos os endereços de e-mail organization.com	`organization.com`
Um utilizador específico	`jdoe@organization.com`
Todos os utilizadores do Gmail	`gmail.com`

Lista negra

A lista negra impede que utilizadores específicos ou grupos de utilizadores se registem no Dell Server ou utilizem o Data Guardian. Os utilizadores cujos endereços de e-mail forem introduzidos na lista negra recebem uma mensagem a declarar que não podem registar-se no Data Guardian.

NOTA:
Se um utilizador já se encontrar registado, esta lista **não** os impede de utilizar o Data Guardian.

Pode utilizar a lista negra para excluir utilizadores específicos que sejam membros de grupos aprovados na lista de acesso total. Além disso, pode colocar domínios completos na lista negra, evitando assim o registo de qualquer pessoa com um endereço de e-mail nesse domínio. Consulte os seguintes exemplos para impedir um utilizador ou grupo de se registar no Dell Server:

Tipo de utilizador	Introduzir
Todos os endereços de e-mail organization.com	`organization.com`
Um utilizador específico e o respetivo endereço de e-mail	`jdoe@organization.com`
Todos os utilizadores do Gmail	`gmail.com`

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

1 No painel esquerdo da Remote Management Console, clique em **Gestão > Gestão de utilizadores externos**.

2 Clique em **Adicionar**.

3 Selecione Tipo de acesso ao registo:

Lista negra - bloqueia o registo de um utilizador ou domínio. O utilizador não pode abrir um documento do Office protegido ou ficheiro .xen.

Lista de acesso total - concede acesso ao registo e a todos os ficheiros para um utilizador ou domínio. Se um utilizador ou domínio também estiverem na lista negra, não é concedido qualquer acesso.

4 No campo Introduzir domínio/e-mail, introduza o domínio do utilizador para definir o acesso a todo o domínio ou o endereço de e-mail para definir o acesso apenas a esse utilizador.

5 Clique em **Adicionar**.

Para obter mais informações sobre como utilizar a lista de acesso total/lista negra, consulte *AdminHelp*, acessível a partir da Remote Management Console no Dell Server.

Um utilizador externo pode solicitar o acesso a um utilizador interno através da chave de um ficheiro protegido. Se o utilizador interno não estiver disponível, pode utilizar a Consola de Gestão Remota para aprovar ou recusar o acesso.

1 Selecione **Gestão > Gestão de pedidos de chave**.

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

Tarefas do cliente

Pré-requisitos

- Certifique-se de que os dispositivos de destino estão ligados a:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Certifique-se de que o utilizador que executar a instalação tem uma conta local de administrador.
- Se efetuar a instalação através de uma linha de comandos, certifique-se de que possui o nome de domínio totalmente qualificado do Security Server que os utilizadores ativarão.

Melhores práticas

Durante a implementação, certifique-se de que segue as melhores práticas de TI. Isto inclui, mas não se limita a:

- Ambientes de testes controlados para testes iniciais
- Implementações escalonadas para utilizadores

Cliente de instalação

Neste ponto, os utilizadores que foram adicionados à lista branca podem registar-se em: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Depois do registo, o utilizador recebe um e-mail que o direciona para https://yoursecurityservername.domain.com:8443/cloudweb, de forma a iniciar sessão e transferir o cliente adequado.

A instalação do cliente Mac é opcional para administradores, uma vez que os utilizadores finais instalam normalmente o cliente Mac (após o registo) eles próprios a partir de https://yoursecurityservername.domain.com:8443/cloudweb.

No entanto, pode instalar o cliente Mac se a sua organização exigir que o faça. Instale o cliente Data Guardian através da interface do utilizador ou através da linha de comandos, utilizando qualquer tecnologia push disponível na sua organização. O registo e a ativação pelo utilizador final continuam a ser necessários.

Atualização de versões anteriores do Cloud Edition

Se uma empresa tiver uma versão anterior do Cloud Edition e atualizações do Data Guardian, a versão anterior do Cloud Edition é removida.

NOTA:
Se a empresa atualizar do Cloud Edition para o Data Guardian, os utilizadores têm de efetuar novamente a autenticação e a ligação do Data Guardian ao respetivo fornecedor de armazenamento em nuvem. Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

Opções de instalação

Para instalar/atualizar o cliente, selecione o seguinte:

- Instalação interativa - Este é o método mais fácil de instalar o Data Guardian para Mac. No entanto, utilize este método apenas se planear instalar o cliente num computador de cada vez.

  ou

- Instalação através da linha de comandos - Para este método de instalação avançado, os administradores têm de ter experiência na sintaxe da linha de comandos. Este método pode ser utilizado para uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na sua organização.

Instalação interativa

1. Para o cliente Data Guardian, localize o programa de instalação em **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilize o ficheiro **.pkg** dentro de DDPSL-Explorer-0.x.x.xxxx.dmg para efetuar a instalação ou atualização. Pode utilizar uma instalação com script, ficheiros de batch ou qualquer outra tecnologia disponível na 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 **Aceito** para continuar.
8. Na janela Tipo de configuração, selecione **Dell Management Server no local**.

   NOTA:
   O *Hosted Dell Security Center* destina-se a um lançamento futuro.

9. Na janela Tipo de instalação, efetue um destes passos:
   - Clique em **Instalar** e, em seguida, avance para o passo 9.
   - Clique em **Alterar local de instalação**.
     1. Na janela de seleção de destino, selecione todos os utilizadores ou um único utilizador.
     2. Clique em **Continuar**.
     3. Clique em **Instalar** e, em seguida, avance para o passo 9
10. Na caixa de diálogo, introduza o seu nome e a sua palavra-passe e clique em **Instalar software**.
11. Na janela Resumo, clique em **Fechar**.
12. Consulte Ativação do utilizador final.

    NOTA:
    Se a empresa atualizar do Cloud Edition para o Data Guardian, os utilizadores têm de efetuar novamente a autenticação e a ligação do Data Guardian ao respetivo fornecedor de armazenamento em nuvem. Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

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

Instalação com linha de comandos

1. Monte o .dmg.
2. Execute a instalação do pacote a partir da linha de comandos através do comando instalador:

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

3 Instrua os utilizadores para ativarem o Data Guardian. Consulte Ativação do utilizador final.

Ativação do utilizador final

Depois de abrir o Dell Data Guardian no Mac pela primeira vez, siga estes passos:

1 No Finder, selecione **Aplicações** e faça duplo clique em **Dell Data Guardian**.
2 Quando abrir a janela do Dell Server, introduza o endereço do Dell Server e, em seguida, clique em **Guardar**.

É aberta a janela Credenciais.

3 Introduza o endereço de e-mail do seu domínio e palavra-passe do domínio.
4 Clique em **Iniciar sessão** para ativar o Dell Data Guardian.

Quando a aplicação Dell Data Guardian for aberta e a ativação for bem-sucedida, o nome do fornecedor de armazenamento em nuvem é apresentado no painel esquerdo.

Se uma empresa pretender que todos os utilizadores colaborem através do mesmo fornecedor de armazenamento em nuvem, o administrador pode definir uma política para permitir apenas esse fornecedor e bloquear a apresentação de outros.

Se a autenticação para o Dell Data Guardian for revogada ou expirar, o nome do fornecedor de armazenamento em nuvem também se apresenta a cinzento.

5 No painel à esquerda, selecione o fornecedor de armazenamento na nuvem.

É aberta uma janela e ser-lhe-ão solicitadas as suas credenciais. Depois de autenticado, o nome do fornecedor de armazenamento em nuvem é ativado.

6 Para obter mais informações sobre autenticação, consulte a Ajuda do Dell Data Guardian.

Desinstalar o Data Guardian

Esta secção descreve o processo de administrador de desinstalação do Data Guardian. Para realizar a desinstalação, tem de ter uma conta de administrador. Se um utilizador final tiver uma conta de administrador local, pode desinstalar o Data Guardian para Mac.

Execute um dos seguintes passos para remover o Data Guardian:

Finder

1 Enquanto prime a tecla <opção>, selecione **Ir** na barra de menu.
2 Abra a pasta **~/Biblioteca/Application Support/Dell**.
3 Clique com o botão direito do rato na pasta **DellDataGuardian** e selecione **Mover para a reciclagem**.
4 A partir de **Ir** na barra de menu, abra a pasta Aplicações e mova a aplicação **Dell Data Guardian** para a Reciclagem.
5 Clique em **OK**.
6 Se for solicitado, introduza a palavra-passe de administrador.

Terminal

Pode ter o Data Guardian num ou em ambos dos seguintes locais.

1 Utilize os seguintes comandos:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Elimine a pasta **DellDataGuardian**.

5

Configurar e instalar o Data Guardian no cliente Web

Este cliente Web permite aos utilizadores visualizarem um documento do Office ou um ficheiro .xen protegido sem instalar o cliente Data Guardian. Como regra geral, a Dell recomenda instalar primeiro o Security Management Server ou o Security Management Server Virtual.

Transferir o ficheiro OVA

Durante a instalação inicial, o Data-Guardian-Web é fornecido como um ficheiro OVA (Open Virtual Application), uma aplicação utilizada para o fornecimento de software executado numa máquina virtual.

Para transferir o ficheiro OVA:

1 Navegue para a página de apoio técnico do Data Guardian.
2 Clique em **Controladores e transferências**.
3 Em seguida "Ver todas as atualizações disponíveis para <versão OS>," clique em **Alterar OS**, e selecione um dos seguintes: **VMware ESXi 6.0** ou **VMware ESXi 5.5**.
4 Em "Ver por:" selecione **Mostrar tudo**.
5 Em Dell Data Security, selecione **Transferir**.

Instalar Data Guardian para Web

Instalar e configurar o Data-Guardian para Web

Antes de começar, certifique-se de que todos os Requisitos de sistema e de ambiente virtual sejam atendidos.

1 Localize os ficheiros do Data Guardian no suporte multimédia de instalação e faça duplo clique em **Data-Guardian-Web-1.x.x.ova** para importar para a VMware.
2 Ligue o Data-Guardian para Web.
3 Selecione o idioma do contrato de licença e selecione **Apresentar EULA**.
4 Leia o contrato e selecione **Aceitar EULA**.
5 Se estiver disponível uma atualização, selecione **Aceitar**.
6 No pedido de alteração da palavra-passe predefinida, selecione **Sim**.
7 No ecrã *Definir a palavra-passe ddguser*, introduza a palavra-passe atual (predefinida), **ddguser** e, de seguida, introduza uma palavra-passe única, volte a introduzir a palavra-passe única e selecione **OK**.

   As palavras-passe devem incluir o seguinte:

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

8 Repita o passo anterior para as contas *ddgconsole* e *ddgsupport*.

NOTA:
Para manter a palavra-passe predefinida, que é igual ao nome, clique em **Cancelar**. Para modificar a palavra-passe, introduza **ddgconsole** ou **ddgsupport** no campo da palavra-passe atual.

9 Na caixa de diálogo *Configurar o nome de anfitrião*, utilize a tecla de retrocesso para remover o nome de anfitrião predefinido. Introduza um nome do anfitrião FQDN e selecione **OK**.

10 Se tiver vários nós e um balanceador de carga, introduza um nome do anfitrião do balanceador de carga.

11 No ecrã *Configurar definições de rede*, escolha uma das opções abaixo e selecione **OK**.

- (Predefinida) Usar DHCP
- (Recomendada) No campo Usar DHCP, prima a Barra de espaços para remover o X e introduzir manualmente estes endereços, conforme aplicável: Static IP Network Mask Default Gateway DNS Server 1 DNS Server 2 DNS Server 3

NOTA:
Ao utilizar um IP estático, também tem de criar uma entrada de anfitrião no servidor DNS.

12 Quando o ecrã scp for apresentado, não clique em OK. Tem de adicionar primeiro os ficheiros .cer e .key à aplicação ou extraí-la do ficheiro .pfx ou .p7b do CA. Consultar Utilizar a ferramenta WinSCP.

NOTA:
Se clicar em OK no ecrã scp antes de extrair estes ficheiros, tem de reiniciar o Data-Guardian para Web e navegar para a caixa de diálogo *Configurar definições de rede*.

Utilizar a ferramenta WinSCP

No Windows, utilize a sua conta do ddgconsole para scp o ficheiro do certificado SSL e o ficheiro de chave SSL.

1 No Windows, abra a ferramenta WinSCP.

2 Na página do WinSCP, introduza o nome do anfitrião.

3 Introduza o nome de utilizador e palavra-passe predefinidos do ddgconsole (ou o nome de utilizador e palavra-passe alterados).

4 Clique em **Início de sessão**.

5 Arraste o certificado e a chave, ficheiro .pfx, ou o ficheiro .p7b da sua unidade local para o diretório **opt/dell/ficheiros**.

6 Se adicionou um ficheiro .pfx ou .p7b, introduza uma palavra-passe quando for solicitado. O certificado e a chave são extraídos do CA e adicionados ao **apache2/ssl/pasta**.

Em alternativa, em vez de arrastar o ficheiro .pfx ou o ficheiro .p7b, pode extrair o certificado manualmente. Apresentamos um código de exemplo:

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

Apresentamos um código de exemplo para extrair a chave privada do ficheiro .pfx:

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

7 Regresse à Consola de administração do ecrã scp.

Consola de administração

Na Consola de administração do ecrã scp:

1 Clique em **OK**. Aparece o ecrã de *Instalação do certificado do proxy inverso Apache2*, apresentando o certificado.

2 Selecione um certificado e prima **Enter**.

3 Proceda da seguinte forma:

- Se adicionou uma chave à ferramenta WinSCP, selecione a chave no ecrã seguinte e prima **Enter**.
- Se introduziu uma palavra-passe na ferramenta WinSCP para um ficheiro .pfx ou .p7b, introduza a palavra-passe quando solicitada e clique em **OK**.

4 No ecrã Definir Dell Server, introduza o nome do anfitrião do servidor e clique em **OK**. É apresentada uma caixa de diálogo com uma lista de URL a ser utilizada quando efetuar aprovisionamentos. O URL está no seguinte formato: **https://node.domain.com/edap-admin-ui/provision_node**.

> **NOTA:**
> **node.domain.com** é o nome introduzido em *Configurar o nome do anfitrião*. O URL aponta para esse nó.

5 Abra um browser e introduza esse URL.

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

7 Na página de início de sessão, introduza o seu domínio, e-mail e palavra-passe e clique em **Iniciar sessão**. A caixa de diálogo do Dell Data Guardian indica que o aprovisionamento foi efetuado com sucesso.

8 Regresse ao ecrã da Consola de administração que incluía o seu URL e clique em **OK**. O servidor da aplicação é reiniciado e a Consola de administração > Menu principal abre-se.

Tarefas adicionais:

- Forneça o URL aos utilizadores internos para lhes permitir o acesso ao cliente Web do Data Guardian.
  - Para um único nó, o URL está neste formato: **https://nodename/** onde nodename reflete o nome do anfitrião introduzido no ecrã *Configurar nome do anfitrião*.
  - Para vários nós, o URL está neste formato: **https://loadBalancerName/** onde nodename reflete o nome do anfitrião do balanceador de carga introduzido no ecrã *Configurar nome do anfitrião*.
- Para aceder ao servidor no futuro para verificar a existência de atualizações para esta VM ou para verificar os registos, o utilizador tem de ativar o SSH para esta VM. Selecione **Configuração básica > Definições de SSH** para ativar o SSH para um utilizador ddgsupport.
- Na Management Console, se modificar qualquer política do portal Web baseada no nó, tem de reiniciar o dispositivo. Consulte Reiniciar o dispositivo. Após o reinício, o utilizador tem de iniciar sessão com as credenciais ddguser.

Abrir a Management Console

Abra a Management Console em https://server.domain.com:8443/webui/

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

Os seguintes browsers são compatíveis com a Management Console:

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

Tarefas de configuração básica do terminal Data Guardian

É possível aceder às tarefas de configuração básicas a partir do menu principal.

Alterar Nome do anfitrião

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar .

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

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

Alterar definições de rede

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar .

1 No menu de *Configuração básica*, selecione **Rede**.
2 No ecrã *Configurar definições de rede*, escolha uma das opções abaixo e selecione **OK**.
   - (Predefinida) Usar DHCP (IPv4).
   - (Recomendada) No campo Usar DHCP, prima a barra de espaços para remover o X e introduzir manualmente estes endereços, conforme aplicável:

     IP estático

     Máscara de rede

     Gateway predefinido

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

     É possível selecionar IPv6 ou IPv4 para uma configuração estática.

NOTA:
Ao utilizar um IP estático, tem de criar uma entrada de anfitrião no servidor DNS.

Alterar palavras-passe de utilizadores

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar .

Pode alterar as palavras-passe para os seguintes utilizadores:

- ddguser (Administrador do terminal) - Este utilizador tem acesso ao terminal Data Guardian e aos respetivos menus.
- ddgconsole (acesso à shell) - Este utilizador tem acesso ao shell Data Guardian. O acesso à shell está disponível para que um administrador de rede verifique e resolva problemas de conetividade da rede.
- ddgsupport (administrador Dell ProSupport) - Este utilizador existe apenas para uso do Dell ProSupport. Por razões de segurança, a palavra-passe desta conta é controlada por si.

1 No menu *Configuração básica*, selecione **Alterar palavras-passe de utilizador**.
2 No ecrã *Alterar palavras-passe de utilizador,* selecione a palavra-passe a alterar e selecione **Enter**.
3 No ecrã *Definir palavra-passe*, introduza a palavra-passe atual, introduza a nova palavra-passe, reintroduza a nova palavra-passe e selecione **OK**.

   As palavras-passe devem incluir o seguinte:

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

NOTA: Para selecionar contas de utilizador diferentes, utilize a barra de espaço no teclado para visualizar a lista de seleção.

Ativar SSH

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar .

Pode ativar o SSH para o início de sessão do administrador de suporte, o acesso à shell e a interface de linha de comandos do terminal.

1 No menu de *Configuração básica*, selecione **SSH**.
2 Realce o utilizador para o qual pretende ativar o SSH, pressione a barra de espaços para introduzir um **X** e selecione **OK**.

Iniciar ou parar serviços

Realize esta tarefa apenas se tal for necessário.

1 Para iniciar ou parar simultaneamente todos os serviços, a partir do menu *Configuração básica*, selecione **Iniciar aplicação** ou **Parar aplicação**.
2 No pedido de confirmação, selecione **Sim**.

NOTA: As alterações ao estado do servidor podem demorar até dois minutos a serem concluídas.

Reiniciar o dispositivo

Realize esta tarefa apenas se tal for necessário.

1 No menu *Configuração básica*, selecione **Reiniciar dispositivo**.
2 No pedido de confirmação, selecione **Sim**.
3 Após o reinício, inicie sessão no Data Guardian.

Encerrar dispositivo

Realize esta tarefa apenas se tal for necessário.

1 No menu *Configuração Básica*, desloque para baixo e selecione **Encerrar dispositivo**.
2 No pedido de confirmação, selecione **Sim**.
3 Após o reinício, inicie sessão no Data Guardian.

Tarefas do administrador

Definir ou alterar o idioma do terminal

Reiniciar os serviços sempre que é realizada uma alteração nas definições constitui uma boa prática.

1 No Menu principal, selecione **Definir idioma**.
2 Utilize as teclas de seta para selecionar o idioma da sua preferência.

Gerar um Registo de Instantâneo do Sistema

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

1 No menu *Ferramentas de suporte*, selecione **Gerar registo de instantâneo do sistema**.
2 Na indicação de que o ficheiro foi criado, selecione **OK**.