Dell Data Guardian

Windows, Mac, dispositivos móviles y guía del administrador web v1.6/1.3

Notas, precauciónes y advertencias

NOTA: Una NOTA señala información importante que lo ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

ADVERTENCIA: Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

Windows, Mac, dispositivos móviles y guía del administrador web

2018 - 05

Rev. A01

Contenido

1

Introducción

Toda la información sobre la política y sus descripciones se encuentran en la AdminHelp.

Antes de empezar

1 Instale Servidor de administración de seguridad/Servidor virtual de administración de seguridad antes de implementar clientes. Localice la guía correcta, tal como se indica a continuación, siga las instrucciones y, a continuación, vuelva a esta guía.

- *Guía de instalación y migración de Dell Servidor de administración de seguridad*
- *Guía de inicio rápido y guía de instalación de Dell Servidor virtual de administración de seguridad*

Compruebe que las políticas están establecidas de la forma deseada. Explore la ayuda AdminHelp, disponible a través del signo **?** que se encuentra en el extremo derecho de la pantalla. AdminHelp es una ayuda a nivel de página diseñada para ayudarlo a definir y modificar las políticas y conocer qué opciones tiene disponibles con Servidor de administración de seguridad/Servidor virtual de administración de seguridad.

2 Lea detenidamente el capítulo Requisitos de este documento.

3 Implemente los clientes en los usuarios finales.

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell 24 horas al día, 7 días a la semana.

De manera adicional, puede obtener soporte en línea para los productos Dell en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport .

2

Requisitos

Servidor

Data Guardian para Windows, Mac y móviles requiere Servidor de administración de seguridad o Servidor virtual de administración de seguridad, v9.6 o posterior. El cliente web Data Guardian requiere Servidor de administración de seguridad o Servidor virtual de administración de seguridad, v9.8 o posterior. A efectos del presente documento, ambos servidores se conocen como Dell Server, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Dell Servidor virtual de administración de seguridad).

Data Guardian para Windows

- Durante la implementación se deberán seguir las prácticas recomendadas para TI. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados, para las pruebas iniciales e implementaciones escalonadas para los usuarios.
- La cuenta de usuario que realiza la instalación/actualización/desinstalación debe ser un usuario administrador local o de dominio, que puede ser designado temporalmente mediante una herramienta de implementación como Microsoft SMS o Dell KACE. No son compatibles los usuarios con privilegios elevados que no sean administradores.
- Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Data Guardian es compatible con versiones específicas de Microsoft Office 2016 y también con Microsoft Office 365 Empresa y Empresa Premium. No es compatible con Office 365 Empresa Essentials.
- Para el cifrado en la nube, el equipo debe tener una unidad de disco (valor de letra) asignable disponible.
- Asegúrese de que los dispositivos de destino pueden conectarse a https://yoursecurityservername.domain.com:8443/cloudweb/register y a https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configuradas cuentas de almacenamiento en nube.

  Si los usuarios desean mantener sus cuentas existentes, deben asegurarse de retirar todos los archivos que quieran conservar *sin cifrar* del cliente de sincronización antes de instalar Data Guardian.
- Los usuarios deberán estar preparados para reiniciar sus equipos una vez que se instale el cliente.
- Data Guardian no interfiere en el comportamiento de los clientes de sincronización. Por lo tanto, los administradores y usuarios finales deben familiarizarse con el funcionamiento de estas aplicaciones antes de implementar Data Guardian. Para obtener más información, consulte el servicio de asistencia de Box en https://support.box.com/home, el servicio de asistencia de Dropbox en https://www.dropbox.com/help o el servicio de asistencia de OneDrive en http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Los documentos protegidos de Office son compatibles con Mozy, una solución complementaria de Data Guardian, también con otros productos de almacenamiento en NFS, correo electrónico y nube.
- Si se está ejecutando Office 2010: si las políticas se han definido para proteger documentos de Office y documentos habilitados para macros, los usuarios deben tener Office 2010 Service Pack 1 o superior (v14.0.6029 o superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar si se ha aplicado un Service Pack al conjunto de aplicaciones de Microsoft Office 2010. Sin esta actualización, no se puede tener acceso a los documentos protegidos. Independientemente de la política, los nuevos documentos de Office no estarán protegidos a menos que la funcionalidad de barrido esté activada. El siguiente barrido convierte los documentos de Office en archivos protegidos, pero los usuarios no pueden tener acceso a ellos sin una versión compatible de Office.
- Aunque Dell Encryption no es necesario, si se usa, el cliente Encryption debe ser v. 8.12 o posterior.
- Data Guardian no es compatible con la herramienta de Restauración del sistema de Windows ni con Windows Insider Preview.
- La redirección de carpetas de Microsoft no es compatible con Data Guardian.
- IPv6 no es compatible con el cifrado en la nube.
- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.

Requisitos previos

Si no se ha instalado todavía, el instalador instala el paquete redistribuible Microsoft Visual C++ 2015 (x86 y x64).

NOTA:

Para los sistemas operativos Windows 7 y Windows 8.1, los equipos deben contar con todas las actualizaciones de Windows. Para obtener más información, consulte https://support.microsoft.com/en-us/help/2919355 y https://support.microsoft.com/en-us/help/2999226.

Se requiere Microsoft .Net 4.5.2 (o una versión posterior) para Data Guardian. Todos los equipos enviados desde la fábrica de Dell vienen con .Net 4.5.2 preinstalado. Sin embargo, si no está instalando en hardware de Dell o si está actualizando Data Guardian en hardware de Dell más antiguo, debería comprobar qué versión de .Net tiene instalada y, si fuera necesario, actualizar la versión antes de instalar Dell Data Guardian, con el fin de evitar errores durante la instalación/actualización. Para comprobar qué versión de .Net tiene instalada, siga estas instrucciones en el equipo en el que se va a realizar la instalación: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar Microsoft .Net Framework 4.5.2, vaya a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware

Los requisitos de hardware mínimos deben cumplir las especificaciones mínimas del sistema operativo. La tabla siguiente explica en detalle el hardware compatible con el cliente de Windows.

Hardware de Windows

- 200 MB de espacio libre en el disco, dependiendo del sistema operativo
- Tarjeta de interfaz de red 10/100/1000 o Wi-Fi
- Protocolo TCP/IP instalado y activado

Si su empresa cifra los datos para el almacenamiento en la nube, su equipo debe tener un carácter alfabético disponible para asignar a una unidad de disco.

Sistemas operativos

La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (32 bits y 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro versión 1607 (Anniversary Update/Redstone 1) mediante la versión 1803 (Spring Creators Update/Redstone 4)

NOTA:

El cliente debe contar con uno de estos sistemas operativos o el sistema se bloqueará. Si es necesario, un ajuste en una clave de registro le permite al administrador anular el bloqueo.

Para tener compatibilidad con Redstone 4, debe actualizar el agente antes de actualizar el sistema operativo.

NOTA:
Data Guardian no es compatible con la Protección contra vulnerabilidades de seguridad de Windows Defender (WDEG, por sus siglas en inglés) en Redstone 3 y versiones posteriores, o con el Kit de herramientas de experiencia de mitigación mejorada (EMET, por sus siglas en inglés) en Redstone 2 y versiones anteriores.

Windows 7 no es compatible con la política de geolocalización para los eventos de auditoría de Data Guardian.

Data Guardian no admite varias versiones de Office en un equipo.

Proveedores del almacenamiento en la nube

La siguiente tabla detalla los proveedores de almacenamiento en la nube compatibles con Data Guardian para Windows. Las actualizaciones de los proveedores de almacenamiento en la nube se lanzan con frecuencia. Dell recomienda probar nuevas versiones con Data Guardian antes de ingresarlas en el entorno de producción.

Proveedores del almacenamiento en la nube

- Dropbox
- Dropbox for Business (solo para Windows)

  NOTA:
  En función de la versión de Dell Server que utilice su empresa, todos los archivos y las carpetas de cuentas personales de Dropbox vinculadas a cuentas empresariales podrían cifrarse.
- Box

  NOTA:
  Box Tools y Box Edit no son compatibles con Data Guardian. Utilizar Box Tools puede causar un error de pantalla azul.
- Google Drive
- OneDrive
- OneDrive for Business
- Unified OneDrive

  NOTA:
  Unified OneDrive es un cliente de sincronización unificado tanto para OneDrive como para OneDrive para la Empresa.

Microsoft Office

Data Guardian admite las siguientes versiones de Office. Sin embargo, debe tener solo una versión instalada de Office.

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1
- Office 2016: versión 1705 aplazada, versión 1708 bianual y versión 1712 mensual

Data Guardian para Mac

A continuación se indica el hardware compatible con el cliente Mac.

Hardware de Mac

- Procesadores Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM
- 10 GB de espacio de disco libre

Sistemas operativos

A continuación se indican los sistemas operativos compatibles.

Sistemas operativos Mac

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.3 - 10.13.4

Proveedores del almacenamiento en la nube

En función de los valores de la política, pueden mostrarse los elementos siguientes en la interfaz de Dell Data Guardian para Mac. El usuario no tiene que descargar ni instalar el cliente de sincronización en la nube.

Proveedores del almacenamiento en la nube

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Aplicación móvil Data Guardian

Lo siguiente enumera los sistemas operativos compatibles con la aplicación móvil Data Guardian.

Sistemas operativos 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

Cliente web Data Guardian

Para habilitar el cliente web Data Guardian, el administrador configura una máquina virtual que aloja al cliente web y lo comunica con Servidor de administración de seguridad o Servidor virtual de administración de seguridad v9.8 o posterior.

Los siguientes entornos virtualizados se pueden usar para implementar el cliente web Data Guardian.

Entornos virtualizados

- VMWare ESXi 6.0
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obtener una lista completa de sistemas operativos de host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
  - Consulte http://pubs.vmware.com/vsphere-60/index.jsp para obtener más información.

- VMWare ESXi 5.5
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obtener una lista completa de sistemas operativos de host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
  - Visite http://pubs.vmware.com/vsphere-55/index.jsp para obtener más información

Navegadores web

Puede utilizar Data Guardian con Internet Explorer, Mozilla Firefox, Google Chrome y Microsoft Edge.

En el caso de los dispositivos Mac, también es compatible el navegador Safari.

Compatibilidad de idiomas

Estos clientes cumplen los requisitos de Multilingual User Interface (MUI) y se pueden configurar en los siguientes idiomas.

Compatibilidad de idiomas

- Inglés (EN)
- Español (ES)
- Francés (FR)
- Italiano (IT)
- Alemán (DE)
- Japonés (JA)
- Coreano (KO)
- Portugués brasileño (PT-BR)
- Portugués europeo (PT-PT)

3

Configurar e instalar Data Guardian en Windows

Configuración del registro del cliente Data Guardian

Esta sección detalla toda la configuración de registro aprobada por Dell ProSupport para equipos cliente locales, con independencia del motivo de la configuración de registro. Si una configuración de registro coincide en dos productos, aparecerá en cada categoría.

Los cambios de registro deben realizarlos únicamente los administradores y es posible que no sean adecuados para todas las situaciones.

- Se pueden aumentar los niveles de registro para ayudar a solucionar problemas. Cree o modifique el siguiente parámetro de registro:

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

  "LogVerbosity"=dword:0x1f (31)

  De manera predeterminada, el nivel de registro es 0xf (15).

  Valores disponibles:

  Desactivado = 0x0 (0)

  Crítico = 0x1 (1)

  Error = 0x3 (3)

  Aviso = 0x7 (7)

  Información = 0xf (15)

  Depuración = 0x1f (31)

- Una vez finalizada la instalación de Data Guardian, los usuarios internos se activan automáticamente. Si es necesario, puede modificar una configuración de registro para invalidar la activación automática.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valor DWORD: DisableAutomaticActivation=1

NOTA:
También puede confirmar los alias para su dominio en Dell Server. Consulte Solución de problemas de activación automática.

Configuración del servidor para Data Guardian

En función de las políticas establecidas por el administrador, Data Guardian protege, por ejemplo, los siguientes datos:

- Los documentos de Office se guardan en una ubicación local, se comparten con otros usuarios de varias formas o se almacenan en medios extraíbles. Pueden protegerse estos tipos de documentos de Office: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.
- Sistemas de uso compartido de archivos basado en la nube: los equipos Windows o los dispositivos móviles capturan datos destinados al almacenamiento en la nube, los cifran y los cargan a la nube.

Informe a los usuarios si su empresa utiliza Data Guardian solo con los documentos de Office, con el almacenamiento en la nube o con ambos.

Configurar Dell Server Virtual para Data Guardian

Si desea configurar Dell Server Virtual para que sea compatible con Data Guardian, en Remote Management Console, active una o ambas políticas de Data Guardian:

- *Documentos de Office protegidos*: solo nivel de empresa
- *Cifrado de nube*: empresa, grupos de extremos o nivel de extremos

Configurar Dell Server para Data Guardian

Si desea configurar Dell Server para que sea compatible con Data Guardian, en Remote Management Console, active una o ambas políticas de Data Guardian:

- *Documentos de Office protegidos*: solo nivel de empresa
- *Cifrado de nube*: empresa, grupos de extremos o nivel de extremos

A continuación, configure el servidor de seguridad para permitir descargas del cliente Cloud.

Configuración del servidor de seguridad para permitir descargas del cliente Data Guardian

Esta sección explica en detalle los pasos a seguir para permitir que los usuarios finales descarguen el cliente Data Guardian de Windows desde su Security Server.

1 En Servidor de administración de seguridad, vaya a **<Security Server install dir>\webapps\root\cloudweb\brand\dell\resources** y abra el **archivo messages.properties** con un editor de texto.

2 Compruebe que las entradas sean las siguientes:

download.deviceWin.mode=remote

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

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

3 Edite las entradas con los siguientes

download.deviceWin.remote.link.32=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<YOUR HOST URL>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe

4 Guarde y cierre el archivo.

5 Vaya a <Directorio de instalación de Security Server> y cree una carpeta nueva dentro con el nombre Download (Security Server \Download).

6 En la carpeta Descarga, cree otra carpeta nueva y denomínela cloudweb (Servidor de seguridad\Descarga\cloudweb).

7 Agregue los archivos de configuración de 64 y 32 bits de Data Guardian a la carpeta cloudweb y cámbieles el nombre si lo desea, por ejemplo, a DataGuardian64.exe y DataGuardian32.exe, respectivamente.

Estos están definidos por el usuario, pero deben coincidir con los nombres de archivo en el documento versions.xml.

8 Reinicie el servidor de seguridad para que los cambios surtan efecto.

Configurar Servidor de administración de seguridad para descargas automáticas del cliente Windows Data Guardian (opcional)

Para las descargas automáticas, el archivo versions.xml y los elementos binarios deben estar en la misma ubicación. La ubicación debe ser accesible para el cliente, por lo que podría ser IIS o podría utilizar la carpeta **Servidor de seguridad\Descarga\cloudweb** que ha creado. En caso de que se utilice la carpeta cloudweb, a continuación se presenta un ejemplo de cómo configurar Dell Server.

1 Vaya a la carpeta **Servidor de seguridad\Descarga\cloudweb**. (Consulte el paso 6 en Configuración del servidor de seguridad para permitir las descargas del cliente Data Guardian.)

2 Cree una carpeta con el nombre DataGuardianUpdate.

> **NOTA:**
> DataGuardianUpdate es solo un ejemplo; puede elegir el nombre que desee.

3 Coloque los ejecutables actualizados en la carpeta DataGuardianUpdate.

4 Cree un archivo *versions.xml* en la carpeta DataGuardianUpdate.

5 Abra el archivo *versions.xml* con un editor de texto y compruebe que la ruta de acceso del nombre del archivo es la correcta para su entorno.

Ejemplo:

```
<?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>
```

Versión: indica la versión del archivo de los ejecutables actualizados

Nombre de archivo setup.exe: el usuario define el nombre de configuración de los archivos ejecutables, pero este debe coincidir con el nombre de configuración del archivo messages.properties. (Consulte el paso 3 en Configuración del servidor de seguridad para permitir las descargas del cliente Data Guardian.)

6 Guarde y cierre el archivo.

7 Agregue los archivos binarios a esta carpeta.

8 Si utiliza IIS, reinicie IIS.

9 Como administrador de Dell, inicie sesión en la Remote Management Console.

10 En el panel izquierdo, haga clic en **Poblaciones** > **Empresa**; se mostrará la pestaña Políticas de seguridad.

11 En el grupo de tecnología Data Guardian, haga clic en **Cifrado en la nube**.

12 Haga clic en **Mostrar la configuración avanzada**.

13 Desplácese hasta la política *URL del servidor de actualización de software* e ingrese **https://<YOUR HOST URL > / DataGuardianUpdate**.

> **NOTA:**
> DataGuardianUpdate es solo un ejemplo que se utiliza para que coincida con la información proporcionada anteriormente.

14 Haga clic en **Guardar** para guardar la modificación de la política en la cola para confirmar.

15 Haga clic en **Administración** > **Confirmar**.

16 Escriba un comentario y haga clic en **Confirmar políticas**.

Recreación de la imagen de un equipo con Data Guardian

Si es necesario recrear la imagen de la computadora de un usuario remoto y este dispone de Data Guardian, pregunte si el usuario ha trabajado sin conexión y creado algún documento de Office protegido en ese tiempo. Si es así, las claves sin conexión que se han generado para esos documentos y esas claves no están custodiadas en Dell Server.

1 Para obtener información sobre cómo recuperar las claves generadas sin conexión de Data Guardian que no se pudieron custodiar en Dell Server, consulte la *Guía de recuperación*.

2 Busque una carpeta de claves sin conexión antes de volver a crear la imagen del equipo del usuario.

Cuando se crean las primeras claves de custodia, se agrega una carpeta de Data Guardian a **C:\Program Files\Dell**. Acceda a la carpeta **Data Guardian > Claves sin conexión**. Si no hay ninguna carpeta de claves sin conexión, compruebe la carpeta **Mis documentos** del usuario.

Desactivar la Protección contra vulnerabilidades de seguridad de Microsoft o EMET para aplicaciones administradas

En Windows 10, se pueden habilitar o compilar las siguientes opciones en el sistema operativo:

- Redstone 3 y versiones posteriores: Protección contra vulnerabilidades de seguridad de Windows Defender (WDEG)
- Redstone 2 y versiones posteriores: Kit de herramientas de experiencia de mitigación mejorada (EMET)

Si se habilitan o se activan estas funciones, debe realizar la configuración para deshabilitar estas aplicaciones administradas para Data Guardian:

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

Protección contra vulnerabilidades de seguridad de Windows Defender (WDEG)

Para desactivar las aplicaciones administradas:

1 Vaya al **Centro de seguridad de Windows Defender**.

2 Haga clic en **Control de las aplicaciones y navegación**.

3 Desplácese hasta la parte inferior de la pantalla y haga clic en **Explotar configuraciones de protección**.

4 Seleccione **Configuración del programa**.

5 Haga clic en **+** para agregar cada aplicación administrada que se muestre en la lista de arriba.

6 En las Propiedades para cada aplicación administrada, seleccione la casilla de verificación *Anular* para cualquier opción que esté en *Activado* y, a continuación, alterne la opción a **Desactivado**.

NOTA:
Si se abre una aplicación administrada y un diálogo establece que debe reestablecer el .exe, reiníciela luego de completar estos pasos.

7 Haga clic en **Aplicar**.

8 Haga clic en **Sí**.

En Configuración del programa, las aplicaciones administradas enumeran las anulaciones en función de las opciones que cambió.

Kit de herramientas de experiencia de mitigación mejorada (EMET)

Para desactivar las aplicaciones administradas:

1 Vaya a **Configuración de la aplicación**.

2 En las opciones de **Verificación ROP de la persona que llama** y **Exportar el filtro de direcciones de la tabla de direcciones (EAF)**, borre las casillas de verificación para las aplicaciones administradas mencionadas anteriormente.

Administrar perfiles de proveedor de protección de almacenamiento en la nube

Data Guardian cifra los archivos de los usuarios y envía eventos de auditoría a Servidor de administración de seguridad/Servidor virtual de administración de seguridad. Para cambiar el comportamiento de cada proveedor admitido de almacenamiento en la nube, establezca cada proveedor con uno de estos valores:

Valor	Descripción
Proteger	Permitir al proveedor/conexión, cifrar los archivos y enviar eventos de auditoría acerca de la actividad del archivo/carpeta.
Bloquear	Bloquear todo el acceso al proveedor/conexión.
Permitir	Permitir al proveedor/conexión que pase sin cifrado, pero con auditoría de la actividad del archivo/carpeta.
Omitir	Omitir la protección del proveedor/conexión sin cifrado o auditoría. Cuando se establece este valor, no se muestra la carpeta del proveedor de almacenamiento en la nube en la unidad virtual Data Guardian del equipo cliente.

Para obtener más información, consulte *AdminHelp*, al que puede acceder desde Remote Management Console de Dell Server.

Permitir o denegar usuarios en la lista de acceso total/lista negra

Determine qué usuarios externos podrán registrarse en Servidor de administración de seguridad/Servidor virtual de administración de seguridad para utilizar Data Guardian. Para mantener la seguridad adecuada, asegúrese de configurar y administrar con cuidado estas listas.

- Un usuario interno se encuentra dentro del dominio.
- Un usuario externo es un usuario que no pertenece al dominio, se trata bien de una persona de otra organización con la que un usuario interno desea compartir documentos empresariales confidenciales o de un usuario interno que quiere acceder a su equipo desde un dispositivo fuera del dominio.

Si desea permitir que un usuario que no pertenece al dominio de la organización se registre para utilizar Data Guardian:

1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración > Administración de usuario externo**.

2 Haga clic en **Agregar**.

3 Seleccione Tipo de acceso al registro:

Lista negra: bloquea el registro de un usuario o un dominio. El usuario no puede abrir un documento de Office o archivo .xen protegido.

Lista de acceso total: permite el registro y el acceso a todos los archivos a un usuario o dominio. Si el usuario o dominio también están en la lista negra, no se le otorgará acceso.

4 En el campo Ingresar dominio/correo electrónico, ingrese el dominio del usuario para otorgar acceso a todo el dominio o la dirección de correo electrónico para otorgar acceso únicamente a ese usuario.

5 Haga clic en **Agregar**.

Para obtener más información sobre el uso de la lista de acceso total/lista negra, consulte *AdminHelp*, accesible desde Remote Management Console de Dell Server.

Instalar Data Guardian

Existen dos métodos para realizar la instalación de Data Guardian:

- Instalación de Data Guardian de forma interactiva
- Instalación de Data Guardian con la línea de comandos

Los usuarios de Data Guardian deben realizar las tareas siguientes para que los archivos y las carpetas de sus clientes de sincronización en la nube estén protegidos. Una vez finalizada la instalación del cliente Data Guardian, los usuarios deben descargar un proveedor de almacenamiento en la nube:

- El administrador debe especificar el proveedor de sincronización en la nube que se va a utilizar.

  O bien

- Proporcionar a los usuarios un vínculo para descargar e instalar Dropbox for Business o OneDrive para la Empresa/Unified OneDrive si su empresa utiliza alguno de estos proveedores. Recuerde que los usuarios de Dropbox for Business deben conectarse a Dropbox for Business a través de Data Guardian.

Carpetas preexistentes con archivos sin cifrar

Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configurada una cuenta de almacenamiento en nube.

Si la cuenta de un proveedor de almacenamiento en la nube está configurada con carpetas sincronizadas con el equipo local antes de la instalación de Data Guardian:

- Los archivos y carpetas preexistentes que se hayan sincronizado en la nube se mantendrán como texto no cifrado.
- Los archivos que agregue a estas carpetas preexistentes se mantendrán como texto no cifrado.
- Los archivos que sincronice desde la nube estarán cifrados

  Si desea cifrar los archivos preexistentes, acceda a la Unidad virtual DDG VDisk (creada durante la instalación de Data Guardian), cree una nueva subcarpeta en el cliente de sincronización en la nube y mueva los archivos preexistentes a dicha carpeta.

  O bien

  Para contenidos de gran tamaño, un administrador puede solicitar temporalmente el Menú administrar carpetas.

Menú Administrar carpetas

Es posible que algunos administradores necesiten compartir temporalmente carpetas de solución de problemas con más de un usuario. Puede solicitar permisos al administrador para la opción Administrar carpetas. Normalmente, se trata de una opción temporal.

Instalación de Data Guardian

Debe ser un administrador local para instalar Data Guardian.

El equipo debe tener una letra alfabética disponible para asignarla a una unidad de disco.

Después de instalar Data Guardian, esté preparado para reiniciar el equipo.

Para instalar Data Guardian:

1 Para descargar el instalador de Data Guardian, vaya a la ubicación especificada por su administrador.
2 En función de su sistema operativo, seleccione el instalador de 32 bits o 64 bits, que normalmente aparece como **setup32.exe** o **setup64.exe**, y cópielo en el equipo local.
3 Haga doble clic en el archivo para iniciar el instalador.
4 Si se muestra un aviso de seguridad, haga clic en **Ejecutar**.
5 Seleccione un idioma y haga clic en **Aceptar**.
6 Si se le solicita que instale el paquete redistribuible Microsoft Visual C++ 2015 o el perfil de cliente Microsoft .NET Framework 4.5.2, haga clic en **Aceptar**.
7 En la ventana de Bienvenida, haga clic en **Siguiente**.
8 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
9 En la pantalla Carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada de **C:\Program Files\Dell\Data Guardian\.**

   En **C:**, no instale Data Guardian en las carpetas de los usuarios o de Windows ni en la raíz de cualquier unidad. Se mostrará un error.
10 En el campo `Nombre de Dell Management Server:`, ingrese el nombre del servidor con el que se comunicará esta computadora, como, por ejemplo, servidor.dominio.com. No es necesario incluir www o http(s). Esta información la proporciona el administrador.

   No desmarque la casilla *Activar verificación de confianza en SSL* a menos que lo indique el administrador.
11 Haga clic en **Siguiente**.
12 En la pantalla Confirmar información de Dell Management Server, confirme si la dirección URL del servidor es correcta. El instalador agrega www o http(s) y el puerto. Haga clic en **Siguiente**.
13 En la ventana Tipo de administración, seleccione esta opción:
   - Usuario interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.
14 Haga clic en **Instalar** para comenzar la instalación.

   Se mostrará una ventana de estado que muestra el progreso de la instalación.
15 Cuando se muestre la pantalla Instalación completa, haga clic en **Finalizar**.
16 Haga clic en **Sí** para reiniciar.

   La instalación de Data Guardian se ha completado.
17 Indique a los usuarios finales que confirmen la activación. El ícono de la bandeja del sistema Data Guardian debería tener una marca de verificación verde  . En función de la manera en que se implemente Data Guardian dentro de la empresa, puede que la activación no sea inmediata. Si no es así, el usuario final debe realizar la activación manualmente. Consulte *Data Guardian User Guide (Guía del usuario de Data Guardian)*.

Instalación de Data Guardian con la línea de comandos

- Los modificadores y parámetros de línea de comandos distinguen entre mayúsculas y minúsculas.
- Asegúrese de incorporar un valor que contenga uno o más caracteres especiales, como un espacio en la línea de comandos, en comillas de escape.
- La siguiente tabla indica los modificadores disponibles para la instalación.

Modificador	Significado
/V	Envía las variables al archivo .msi en setup.exe. El contenido siempre debe ingresarse entre comillas de texto sin formato.
/s	Modo silencioso

Opción	Significado
/QB	Diálogo de progreso con botón **Cancelar** , indica que es necesario reiniciar
/QB!	Diálogo de progreso sin botón **Cancelar**, indica que es necesario reiniciar
/QN	Sin interfaz de usuario

- La tabla a continuación indica los parámetros disponibles para la instalación.

Parámetros
SERVIDOR=<ServerName> (FQDN del servidor Dell para la activación)
EMPRESA=1 (usuario interno)
ACTIVARSSLTRUST=0 (Desactivar la validación de SSL Trust)
REINICIAR=SUPRIMIR (El valor nulo permite la configuración automática, SUPRIMIR desactiva el reinicio)

Ejemplo de línea de comandos

- El siguiente ejemplo instala Data Guardian de forma silenciosa, para un usuario interno, en C:\Biblioteca\Registros\Install.log.

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

Configuración de GPO en la controladora de dominio para habilitar derechos

- Si sus clientes están autorizados por Dell Digital Delivery (DDD), siga estas instrucciones para establecer GPO en la controladora de dominio, a fin de habilitar las autorizaciones (es posible que no sea el mismo servidor que ejecuta Servidor de administración de seguridad/Servidor virtual de administración de seguridad).
- La estación de trabajo debe ser miembro del OU donde se aplica el GPO.

NOTA:
Asegúrese de que el puerto de salida 443 esté disponible para establecer comunicación con Servidor de administración de seguridad/Servidor virtual de administración de seguridad. Si el puerto 443 está bloqueado (por cualquier motivo), la función de autorización no funcionará.

1. En el controlador de dominio para administrar los clientes, haga clic en **Inicio** > **Herramientas administrativas** > **Administración de políticas de grupo**.
2. Haga clic con el botón derecho del mouse en el OU donde se debe aplicar la política y seleccione **Crear un GPO en este dominio**, y **Vincularlo aquí...**
3. Ingrese el nombre del nuevo GPO, seleccione (ninguno) para GPO de inicio de origen y haga clic en **Aceptar**.
4. Haga clic con el botón derecho del ratón en GPO que fue creado y seleccione **Editar**.
5. Se carga el Editor de administración de políticas de grupo. Acceda a **Configuración del equipo** > **Preferencias** > **Configuración de Windows** > **Registro**.
6. Haga clic con el botón derecho del mouse en el registro y seleccione **Nuevo** > **Elemento de registro**. Complete lo siguiente.

   Acción: Crear

   Subárbol: HKEY_LOCAL_MACHINE

   Ruta de la clave: SOFTWARE\Dell\Dell Data Protection

Nombre del valor: Servidor

Tipo de valor: REG_SZ

Datos de valor: <dirección IP de Servidor de administración de seguridad/Servidor virtual de administración de seguridad>

7 Haga clic en **Aceptar**.

8 Cierre sesión y vuelva a iniciarla en la estación de trabajo o ejecute **gpupdate /force** para aplicar la política del grupo.

Desinstalar Data Guardian

- Si el usuario final tiene cuenta de administrador local, puede realizar la desinstalación de Data Guardian. Consulte la *Guía del usuario de Data Guardian* para obtener más información. Esta sección describe el proceso del Administrador para desinstalar Data Guardian.

> **IMPORTANTE: archivos que no son de Office en la Unidad virtual DDG VDisk**
> Antes de desinstalar Data Guardian, mueva algunos archivos importantes a una ubicación fuera de la Unidad virtual DDG VDisk. Cuando Data Guardian ha sido desinstalado una computadora de los usuarios finales, las carpetas y los archivos que están en la nube quedarán cifrados e inaccesibles. Si este usuario final deja la compañía y ningún otro usuario comparte esa carpeta o archivo, los datos estarán seguros, pero no se podrán leer (para ver los archivos, puede volver a instalar Data Guardian).
>
> Los documentos de Office protegidos permanecen cifrados si desinstala Data Guardian. Para descifrar, consulte *Guía de recuperación > Recuperación de Data Guardian*.

Desinstalación con la línea de comandos

- Una vez extraído del instalador maestro, el instalador del cliente Data Guardian puede encontrarse en **C:\Dell \DataGuardian_XXbit_setup.exe**.
- El siguiente ejemplo desinstala de forma silenciosa el cliente Data Guardian.

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

Reinicie el equipo cuando se le solicite.

Uso de Data Guardian con Dropbox for Business

Data Guardian con Dropbox for Business ofrece funciones adicionales a las de Dropbox básico.

Puede establecer políticas para controlar cómo se protegen las carpetas de Dropbox empresariales y personales. Si su empresa permite las cuentas de empresa y personales, los usuarios finales deben comprender cómo funciona el cifrado de cada tipo de cuenta. Consulte Política para cuentas de empresa personales.

Política de cuentas de empresa y personales

En su empresa pueden aplicarse pautas sobre si los miembros del equipo pueden utilizar cuentas de empresa y personales. Además, la empresa puede permitir que solo determinados usuarios tengan cuentas de empresa y personales.

> **NOTA:**
> Si su empresa permite las cuentas de empresa y personales, y un usuario final elige utilizar ambas, debe entender la administración de carpetas de ambos tipos de cuentas.

La siguiente tabla describe el cifrado basado en la configuración de la política *Carpetas personales de cifrado de Dropbox*.

Cifrado	Configuración de política	Consideraciones sobre la implementación
Cifre todos los archivos y carpetas de empresa y personales.	Política > Carpetas personales de cifrado de Dropbox > Establecida en **Seleccionada** (predeterminado)	Antes de implementar Data Guardian, los usuarios deben realizar una copia de seguridad de los archivos empresariales preexistentes en las carpetas de sincronización de almacenamiento en la nube, en ubicaciones situadas fuera de las carpetas sincronizadas. Los usuarios con archivos personales que deben permanecer sin cifrar deben mover esos archivos fuera de las carpetas sincronizadas de empresa o desvincular las cuentas personales de los clientes de sincronización de la empresa. Después de que se haya implementado Data Guardian, los archivos y las carpetas en la nube solo podrán visualizarse en equipos o dispositivos que ejecuten Data Guardian. Si una carpeta personal se cifra accidentalmente, consulte "Descifrar carpetas en una cuenta personal" en la Guía del usuario de Dell Data Guardian.
Cifre todos los archivos y las carpetas de la cuenta de empresa. Permita que los archivos y las carpetas de la cuenta personal permanezcan sin cifrar.	Política > Carpetas personales de cifrado de Dropbox > Establecida en **Sin seleccionar**	Puede utilizar la política opcional Mensaje para cifrar carpetas personales en Dropbox para mostrar un mensaje personalizado que recuerde a los usuarios que **no** guarden archivos de la empresa en cuentas personales, porque esos archivos no estarán protegidos. El mensaje se mostrará en estos momentos. • Cada vez que el usuario inicie la sesión • Cuando el usuario cree o agregue un nuevo archivo o carpeta a una cuenta personal de Dropbox Si establece la política Cifrar carpetas personales en Dropbox en **Falso** para un extremo o grupo de extremos, las cuentas personales de todos los usuarios en esos extremos seguirán sin estar cifradas.

Carpetas personales y de empresa

Si su empresa utiliza Dropbox for Business y permite que los usuarios finales tengan carpetas personales y de empresa, quizá desee ejecutar informes para asegurar que todos los archivos de la empresa tengan la extensión .xen, por si acaso el usuario final copia un archivo confidencial desprotegido en una carpeta de empresa. Consulte Solución de problemas de Data Guardian.

Visualización de informes

La información sobre el entorno de Data Guardian se encuentra disponible en Remote Management Console de Dell Server. Seleccione **Informes > Eventos de auditoría** para los eventos de auditoría relacionados con las carpetas de cliente de sincronización en la nube y los documentos de Office protegidos.

Para los propósitos de supervisión y cumplimiento de los detalles del dispositivo, los detalles de Shield o los eventos de auditoría, consulte **Informes > Administrar informes**.

Para obtener más información, consulte *AdminHelp*, al que puede acceder desde la Remote Management Console.

Solución de problemas de Data Guardian

Utilizar la pantalla Detalles

Puede utilizar la pantalla **Detalles** para resolver problemas. Por ejemplo:

- Si un usuario crea una carpeta pero no se está realizando el cifrado, seleccione **Detalles** > **Archivos** > **Estado de la carpeta** para comprobar el estado.
- Si un usuario final solicita soporte, puede indicarle que configure la pantalla Detalles mejorados y seleccione la pestaña **Detalles** > **Política**. En dicha pestaña aparecen las políticas que se están ejecutando.
- Para solucionar problemas, examine los registros .

Utilizar la pantalla Detalles mejorados

- Mientras mantiene pulsado **<Ctrl><Shift>**, haga clic en el ícono de la bandeja del sistema Data Guardian y, a continuación, seleccione **Detalles**.
- Además de los archivos y las carpetas, se muestra lo siguiente:

  Seguridad: muestra la clave, el tipo de clave y el estado. Este panel ofrece una lista temporal de algunos de los archivos de Office protegidos hasta que se envían a Dell Server. La longitud de tiempo depende del intervalo de sondeo.

  Auditoría: enumera los módulos, el ID de usuario y el tipo de evento. En este registro de auditoría la información se encuentra en cola y, a continuación, será enviada a Servidor de administración de seguridad/Servidor virtual de administración de seguridad a intervalos específicos. El administrador puede ver los **Eventos de auditoría** en el panel izquierdo de la Remote Management Console para la auditoría.

  Política: enumera los nombres y valores de la política.

Ver archivos de registro

- Haga clic en **Ver Registro** de la esquina inferior izquierda de la pantalla Detalles.

  Los archivos de registro también se encuentran en **C:\ProgramData\Dell\Data Guardian**.

  Los archivos de registro de documentos de Office protegidos se encuentran en la carpeta Custom.xml.

Solución de problemas de activación automática

Si Data Guardian no se activa automáticamente para varios usuarios, puede cambiar la configuración de registro del cliente Data Guardian. También debe comprobar los alias en Dell Server:

1 En la Remote Management Console, vaya a **Poblaciones > Dominios**, y seleccione un dominio y sus subdominios.
2 En la página Detalles del dominio, seleccione la pestaña **Configuración**.
3 En el campo *Alias*, confirme que todos los alias son correctos.

Proporcionar derechos temporales de administración de carpetas

Puede conceder derechos temporales para administrar carpetas a un administrador o usuario. Por ejemplo, si los usuarios cargaron los archivos a la nube antes de la instalación de Data Guardian, puede proporcionar derechos de administración de la carpeta temporales a algunos usuarios para que administren el cifrado carpeta a carpeta en las carpetas del cliente de sincronización.

Para proporcionar derechos de administración de carpetas:

1 En la Remote Management Console, haga clic en **Poblaciones** > **Extremos**.

2 Busque o haga clic en un extremo y, a continuación, haga clic en la ficha **Políticas de seguridad**.

3 Seleccione **Cifrado en la nube** y luego haga clic en **Mostrar configuración avanzada**.

4 Haga clic en la casilla situada junto a *Administración de carpetas habilitada* para seleccionar la política.

5 Haga clic en **Guardar**.

6 En el panel izquierdo, haga clic en **Administración** > **Confirmar**.

7 Escriba un comentario y haga clic en **Confirmar políticas**.

NOTA:

Dell recomienda que después de cifrar las carpetas o completar la solución de problemas, deje en blanco la casilla de la política *Administración de carpetas habilitada* para desactivar la política en ese extremo.

Para administrar carpetas en el extremo:

1 Cree una carpeta dentro de la carpeta del cliente de sincronización y agregue archivos, de modo que los archivos queden cifrados en la nube.

2 Haga clic en el ícono de la bandeja del sistema Data Guardian y seleccione **Administrar carpetas**.

Para cada cliente de sincronización, se muestra una vista jerárquica de las carpetas sincronizadas en la nube. Todas las carpetas se encuentran seleccionadas de manera predeterminada. Desmarque las carpetas que no desea cifrar. Si anula la selección de una carpeta en Administrar carpetas, un barrido de descifrado descifrará los archivos existentes en esa carpeta. Los nuevos archivos de esa carpeta no estarán cifrados en la unidad local o en la nube.

NOTA:

Si arrastra un archivo cifrado a una carpeta que no se encuentra seleccionada en Administrar carpetas, bien en la nube, bien en la unidad virtual Data Guardian, el archivo permanecerán cifrado y no podrá visualizar el contenido. Además, si comparte la carpeta con otro usuario de Data Guardian que no tenga la política Administrar carpetas habilitada, los archivos se mantendrán cifrados para él y no podrá visualizarlos.

3 Si desea cifrar una carpeta ya existente, active el cifrado para esa carpeta manualmente. Los archivos se cifrarán cuando se sincronicen en la nube.

Preguntas más frecuentes

Preguntas más frecuentes de administración de carpetas

Pregunta

Tengo una carpeta con archivos que he compartido con otro usuario. En la bandeja del sistema, he utilizado la utilidad **Data Guardian > Administrar carpetas** para desproteger el contenido de esa carpeta. Recientemente, mis archivos vuelven a estar cifrados en la nube. Esa carpeta ya no se muestra en la utilidad Administrar carpetas, por lo que ya no puedo descifrar esos archivos en la nube.

Respuesta

Una Id. de clave de cifrado está asociado con una carpeta basada en el primer usuario que agregó un archivo en esa carpeta. Si un usuario crea una carpeta y no agrega archivos, su clave no se asocia a esa carpeta. El usuario cuya Id. de clave de cifrado se ha definido en la carpeta es el único que puede ver la carpeta en la utilidad Administrar carpetas. Si el usuario con ID de clave de cifrado asociado a la carpeta la desmarca en la utilidad Administrar carpetas y la comparte con otro usuario de Data Guardian, el segundo usuario de Data Guardian volverá a cifrar el contenido.

Solución

1 Cree una nueva carpeta.

2 Mueva todos los archivos que desee cifrar a la nueva carpeta.

3 En la bandeja del sistema, use la utilidad **Dell Data Guardian** > **Administrar carpetas** para descifrar esos archivos.

NOTA:
Si descifra el contenido de una carpeta que se comparte con otros usuarios de Data Guardian, el cliente Data Guardian forzará la ejecución de la política para cifrarlos. La práctica recomendada es utilizar la utilidad Administrar carpetas para descifrar solo los archivos que no se comparten con otros usuarios de Data Guardian.

Pregunta

Estoy sincronizando una carpeta descifrada que he desmarcado con la utilidad Administrar carpetas. Sin embargo, cuando intento cargarla mediante el navegador web, solo puedo cargar archivos cifrados.

Respuesta

Data Guardian no se ha diseñado para buscar activamente carpetas en la nube. En el caso de carpetas sin cifrar, Data Guardian puede sincronizarse mediante el cliente de sincronización porque controla el entorno. Es necesario que los archivos que se envían a través del explorador web estén protegidos.

Solución

Agregue archivos a la carpeta de sincronización.

Pregunta

Recientemente desinstalé mi sistema de archivos compartidos basado en la nube desde mi equipo, pero cuando abrí la utilidad Administrar carpetas, uno de los clientes de sincronización todavía estaba incluido como una opción.

Respuesta

Data Guardian no supervisa la instalación o desinstalación del software de terceros. Esas opciones siguen en la lista porque, por diseño, cuando se desinstalan estos clientes, no quitan los archivos existentes. Esos archivos siguen estando protegidos por Data Guardian, a pesar de que el cliente de sincronización ya no está instalado.

Solución

Para eliminar la opción del cliente de sincronización desinstalado de la utilidad Administrar carpetas, mueva las carpetas o los archivos que desea conservar fuera de la carpeta de sincronización, y, a continuación, elimine la carpeta. Después de eliminar la carpeta, esta ya no estará incluida en la utilidad Administración de carpetas.

Otras preguntas más frecuentes

Pregunta

Un usuario dispone de Data Guardian con Documentos de Office protegidos y no puede copiar o pegar.

Respuesta

Para Data Guardian, algunas funciones se controlan desde la bandeja del sistema. Compruebe si el usuario ha modificado la bandeja del sistema.

Solución

Debe utilizarse la configuración predeterminada de la bandeja del sistema. El usuario debe conservar la configuración predeterminada de la bandeja del sistema.

Pregunta

Cambié la política **Ofuscación de nombres de archivos** de GUID a Solo Extensión. Sin embargo, las carpetas que había sincronizado anteriormente siguen cifrando esos archivos en el formato previo, con nombres de archivos GUID. ¿Por qué?

Respuesta

Cuando se cambia una política en Servidor de administración de seguridad/Servidor virtual de administración de seguridad, Data Guardian mantiene la política anterior de esa carpeta. Todas las carpetas nuevas tendrán la nueva política aplicada y se cifrarán en el formato **Solo extensión**.

Solución

Para volver a aplicar el formato **Solo extensión** a los archivos previos, cópielos y péguelos en una nueva carpeta a la que se le haya aplicado la nueva política.

4

Configurar e instalar Data Guardian en Mac

Data Guardian para Mac está diseñado para compartir archivos en proveedores de cifrado en la nube. Sin embargo, si las políticas "Documentos de Office protegidos" están activadas para computadoras Mac, se perderán todas las auditorías y seguimientos de archivos si el usuario final guarda el archivo en la computadora Mac local. Si se necesitan auditorías y seguimientos de archivos estrictos en la organización, establezca la política *Permitir activación de Data Guardian en Mac* en **No seleccionado** para evitar que Data Guardian se active en Mac.

Tareas del servidor

Requisitos previos

Antes de llevar a cabo estas tareas, confirme lo siguiente:

- Instale Dell Server y sus componentes. Consulte una de las opciones siguientes:
  - *Guía de instalación y migración de Servidor de administración de seguridad*
  - *Guía de inicio rápido y guía de instalación de Servidor virtual de administración de seguridad*
- En la Remote Management Console, asigne un rol de administrador de Dell pertinente.

Políticas

De manera predeterminada, Data Guardian cifra los archivos de los usuarios y envía eventos de auditoría a Servidor virtual de administración de seguridad. A efectos del presente documento, ambos servidores se citan como Dell Server, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Servidor virtual de administración de seguridad).

Si desea que los eventos de auditoría incluyan datos de geolocalización, debe activar la Wifi. Para obtener más información sobre la geolocalización y los eventos de auditoría, consulte *AdminHelp*.

Para cambiar el comportamiento predeterminado para cada proveedor de almacenamiento en la nube, configure la política *Proveedores de protección del almacenamiento en la nube*. Si su empresa prefiere un proveedor específico de almacenamiento en la nube, establezca la política en **Bloquear** para otros proveedores. Para obtener información acerca de las políticas, consulte *AdminHelp*, al que puede acceder desde Remote Management Console de Dell Server.

NOTA:
La opción Omitir de la política es para Windows. Si se selecciona Omitir para Mac, se muestra como Permitir para el usuario final.

Configuración del servidor de seguridad para permitir que el cliente realice descargas desde la nube

Antes de llevar a cabo estas tareas, confirme lo siguiente:

- Instale Dell Server y sus componentes. Consulte una de las opciones siguientes:
  - *Guía de instalación y migración de Servidor de administración de seguridad*
  - *Guía de inicio rápido y guía de instalación de Servidor virtual de administración de seguridad*
- En la Remote Management Console, asigne un rol de administrador de Dell pertinente.

Servidor de administración de seguridad

1. En Servidor de administración de seguridad, vaya a <Directorio de instalación de Security Server>\webapps\cloudweb\brand\dell\resources\
2. Abra el archivo **messages.properties** con un editor de texto.
3. Compruebe que las entradas sean las siguientes.
   Para la instalación local:

   download.deviceWin.mode=local

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

   Para la instalación **remota**:

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

   ```
   download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
   ```
4. Guarde y cierre los archivos.
5. Vaya a <Directorio de instalación de Security Server> y cree una carpeta con el nombre Download (Security Server\Download).
6. En la carpeta Download, cree una carpeta CloudWeb (Security Server\Download\CloudWeb).
7. Agregue los instaladores de Dell Data Guardian a dicha carpeta.

Virtual Edition: instalación manual de una versión del cliente de nube diferente

No se requiere ninguna acción para permitir que los usuarios descarguen el instalador de Dell Data Guardian más reciente. El instalador más reciente está preinstalado en el servidor de seguridad Servidor virtual de administración de seguridad.

Para instalar manualmente una versión del instalador de Data Guardian diferente en Servidor virtual de administración de seguridad Security Server, actualice el archivo message.properties.

1. Vaya a:
   /opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2. Abra el archivo **messages.properties** con un editor de texto.
   Para la instalación local:

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

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

   Para la instalación **remota**:

   download.deviceWin.mode=remote

   ```
   download.deviceMac.remote.link=https://[MachineName:IPaddress]:[port]/yourpath/filename.dmg
   ```

3 Guarde y cierre los archivos.
4 Copie los archivos en /opt/dell/server/security-server/download/cloudweb.
5 Agregue los instaladores de Data Guardian a esa carpeta.

Permitir o denegar usuarios en la lista de acceso total/lista negra

Las entradas en las listas negras y de acceso total determinan qué usuarios pueden registrarse en Dell Server para utilizar Data Guardian.

Lista de acceso total

La lista de acceso total permite a usuarios o grupos de usuarios específicos registrarse en Dell Server y utilizar Data Guardian.

Los usuarios externos se deben colocar en la lista de acceso total para permitir el registro. Consulte los ejemplos siguientes para permitir que los usuarios se registren:

Tipo de usuario	Ingresar
Todas las direcciones de correo electrónico tipo organizacion.com	`organization.com`
Un usuario específico	`jdoe@organization.com`
Todos los usuarios de Gmail	`gmail.com`

Lista negra

La lista negra evita que usuarios o grupos de usuarios específicos se registren en Dell Server y utilicen Data Guardian. Los usuarios de correos electrónicos que se ingresen en la lista recibirán un mensaje en el que se les informará de que no podrán registrarse en Data Guardian.

NOTA:
Si un usuario ya está registrado, esta lista **no** le impedirá utilizar Data Guardian.

Puede usar la lista negra para excluir a ciertos usuarios que forman parte de grupos aprobados en la lista de acceso total. Además, puede incluir dominios enteros en la lista negra, para evitar el registro de cualquiera que tenga un correo electrónico de ese dominio. Consulte los ejemplos siguientes para impedir que un usuario o un grupo se registren en Dell Server:

Tipo de usuario	Ingresar
Todas las direcciones de correo electrónico tipo organizacion.com	`organization.com`
Un usuario específico y su dirección de correo electrónico	`jdoe@organization.com`
Todos los usuarios de Gmail	`gmail.com`

Para modificar la lista de acceso total/lista negra, siga estas instrucciones:

1 En el panel izquierdo de la Remote Management Console, haga clic en **Administración > Administración de usuario externo**.
2 Haga clic en **Agregar**.
3 Seleccione Tipo de acceso al registro:

Lista negra: bloquea el registro de un usuario o un dominio. El usuario no puede abrir un documento de Office o archivo .xen protegido.

Lista de acceso total: permite el registro y el acceso a todos los archivos a un usuario o dominio. Si el usuario o dominio también están en la lista negra, no se le otorgará acceso.

4 En el campo Ingresar dominio/correo electrónico, ingrese el dominio del usuario para otorgar acceso a todo el dominio o la dirección de correo electrónico para otorgar acceso únicamente a ese usuario.

5 Haga clic en **Agregar**.

Para obtener más información sobre el uso de la lista de acceso total/lista negra, consulte *AdminHelp*, accesible desde Remote Management Console de Dell Server.

Los usuarios externos pueden solicitar el acceso de un usuario interno a la clave de un archivo protegido. Si el usuario interno no está disponible, puede utilizar la Remote Management Console para aprobar o denegar el acceso.

1 Seleccione **Administración > Administración de solicitudes de claves**.

2 Para obtener más información, seleccione **?** (Ayuda).

Tareas del cliente

Requisitos previos

- Asegúrese de que los dispositivos de destino pueden conectarse a:
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Asegúrese de que el usuario que lleva a cabo la instalación tenga cuenta de administrador local para instalar.
- Si la instalación se hace con la línea de comandos, asegúrese de que tiene el nombre de dominio completo de Security Server en el que los usuarios se activarán.

Prácticas recomendadas

Durante la implementación, asegúrese de que sigue los métodos recomendados para TI. Esas prácticas incluyen, pero sin limitarse a:

- Entornos de prueba controlados para las pruebas iniciales.
- Implementaciones escalonadas para los usuarios.

Instalación del cliente

En este punto, los usuarios que se agregaron a la lista blanca pueden registrase en: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Tras registrarse, el usuario recibe un correo electrónico que le dirige a https://yoursecurityservername.domain.com:8443/cloudweb para que inicie sesión y se descargue el cliente apropiado.

La instalación del cliente Mac es opcional para los administradores, ya que los usuarios finales suelen instalar el cliente Mac ellos mismos (después del registro) desde https://yoursecurityservername.domain.com:8443/cloudweb.

No obstante, puede instalar el cliente Mac si su organización lo considera necesario. Instale el cliente de Data Guardian mediante la interfaz de usuario o la línea de comandos, utilizando cualquier tecnología de inserción que esté disponible en su organización. El registro y la activación por parte del usuario final siguen siendo necesarios.

Actualización desde versiones anteriores de Cloud Edition

Si una empresa tiene una versión anterior de Cloud Edition y actualiza a Data Guardian, se elimina la versión anterior de Cloud Edition.

NOTA:
Si una empresa actualiza de Cloud Edition a Data Guardian, los usuarios deben autenticarse y volver a vincular Data Guardian con su proveedor de almacenamiento en la nube. Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

Opciones de instalación

Para instalar/actualizar el cliente, seleccione una de las opciones siguientes:

- Instalación interactiva: este es el método más sencillo para instalar Data Guardian para Mac. No obstante, utilice este método si únicamente tiene previsto instalar el cliente en un equipo cada vez.

  O bien

- Instalación con la línea de comandos: para este método avanzado de instalación, los administradores deben tener experiencia en sintaxis de la línea de comandos. Este método puede utilizarse para una instalación con secuencia de comandos, utilizando archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.

Instalación interactiva

1. Para el cliente de Data Guardian, localice el instalador en **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilice el archivo **.pkg** almacenado en DDPSL-Explorer-0.x.x.xxxx.dmg para la instalación o actualización. Puede utilizar una instalación con secuencia de comandos, archivos por lotes o cualquier otra tecnología de inserción que esté disponible en su organización.
3. Haga doble clic en el paquete **Dell-Data-Guardian-x.x.x**.
4. Haga clic en **Continuar**.
5. En la ventana Introducción, haga clic en **Continuar**.
6. En la ventana Contrato de licencia de software, haga clic en **Continuar**.
7. Haga clic en **Aceptar** para continuar.
8. En la ventana Tipo de instalación, realice una de estas acciones:
   - Haga clic en **Instalar** y, a continuación, vaya al paso 9.
   - Haga clic en **Cambiar ubicación de instalación**.
     1. En la ventana de Selección de destino, elija todos los usuarios o uno solo.
     2. Haga clic en **Continuar**.
     3. Haga clic en **Instalar**; a continuación, vaya al paso 9
9. En el diálogo, ingrese su nombre de usuario y contraseña y haga clic en **Instalar software**.
10. En la página Resumen, haga clic en **Cerrar**.
11. Consulte Activación del usuario final.

    NOTA:
    Si una empresa actualiza de Cloud Edition a Data Guardian, los usuarios deben autenticarse y volver a vincular Data Guardian con su proveedor de almacenamiento en la nube. Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

12. Cierre la ventana de .dmg para abrir el Buscador.

Instalación con la línea de comandos

1. Monte el .dmg.
2. Utilice el comando de instalación para realizar la instalación del paquete con la línea de comandos:
   ```
   sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
   ```
3. Indique a los usuarios finales que activen Data Guardian. Consulte Activación del usuario final.

Activación del usuario final

Después de abrir Dell Data Guardian en el Mac por primera vez, siga estos pasos:

1 En Finder, seleccione **Aplicaciones** y haga doble clic en **Dell Data Guardian**.
2 Cuando se abra la ventana Dell Server, ingrese la dirección de Dell Server y haga clic en **Guardar**.

Se abrirá la ventana Credenciales.

3 Ingrese la dirección de correo electrónico y la contraseña de su dominio.
4 Haga clic en **Inicio de sesión** para activar Dell Data Guardian.

Cuando se abre la aplicación Dell Data Guardian y se realiza correctamente la activación, el nombre del proveedor de almacenamiento en la nube aparecerá descolorido en el panel de la izquierda.

Si una empresa desea que todos los usuarios colaboren con el mismo proveedor de nube, el administrador puede establecer una política para permitir solo dicho proveedor y bloquear la visualización del resto.

Si se revoca la autenticación para la aplicación Dell Data Guardian o esta caduca, también se desactivará el nombre del proveedor de almacenamiento en la nube.

5 En el panel de la izquierda, seleccione el proveedor de almacenamiento en la nube.

Se abrirá una ventana en la que se le solicitarán sus credenciales. Cuando se autentica, se activa el nombre del proveedor de almacenamiento en la nube.

6 Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

Desinstalar Data Guardian

Esta sección describe el proceso del Administrador para desinstalar Data Guardian. Debe tener una cuenta de administrador local para realizar la desinstalación. Si el usuario final tiene cuenta de administrador local, puede realizar la desinstalación de Data Guardian para Mac por sí mismo.

Lleve a cabo una de estas acciones para quitar Data Guardian:

Finder

1 Mientras mantiene pulsada la tecla <opción>, seleccione **Ir** en la barra de menú.
2 Abra la carpeta **~/Library/Application Support/Dell**.
3 Haga clic con el botón derecho del mouse en la carpeta **Dell DataGuardian** y seleccione **Mover a papelera**.
4 En **Ir** en la barra de menú, abra la carpeta Aplicaciones y mueva la aplicación **Dell Data Guardian** a la Papelera.
5 Haga clic en **Aceptar**.
6 Si se le solicita, ingrese la contraseña del administrador.

Terminal

Es posible que tenga Data Guardian en una o en las dos ubicaciones que se muestran a continuación.

1 Utilice estos comandos:
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian
2 Elimine la carpeta **Dell DataGuardian**.

Configurar e instalar Data Guardian para el cliente web

Este cliente web permite a los usuarios ver un documento de Office protegido o un archivo .xen sin instalar el cliente Data Guardian. Como regla general, Dell recomienda instalar primero Servidor de administración de seguridad o Servidor virtual de administración de seguridad.

Descargar el archivo OVA

En la instalación inicial, Data-Guardian-Web se entrega como un archivo OVA, una Aplicación virtual abierta utilizada para entregar software que se ejecuta en una máquina virtual.

Para descargar el archivo OVA:

1 Vaya a la página Asistencia para productos de Data Guardian.
2 Haga clic en **Controladors y descargas.**
3 Junto a "Ver todas las actualizaciones disponibles para <versión del sistema operativo>", haga clic en **Cambiar SO** y seleccione una de las siguientes opciones: **VMware ESXi 6.0** o **VMware ESXi 5.5**.
4 Bajo "Ver por:" seleccione **Mostrar todo**.
5 En Dell Data Security, seleccione **Descargar**.

Instalar Data Guardian para web

Instalación y configuración de Data-Guardian-Web

Antes de comenzar, asegúrese de que se cumplan todos los Requisitos de los entornos virtualizados y del sistema.

1 Localice los archivos de Data Guardian en el medio de instalación y haga doble clic en **Data-Guardian-Web-1.x.x.ova** para importarlos a VMware.
2 Encender Data-Guardian-Web.
3 Seleccione el idioma para el contrato de licencia y, a continuación, seleccione **Mostrar CLUF**.
4 Lea el contrato y seleccione **Aceptar CLUF**.
5 Si hay una actualización disponible, seleccione **Aceptar**.
6 En la solicitud de cambio de contraseña predeterminada, seleccione **Sí**.
7 En la pantalla *Establecer contraseña ddguser*, ingrese la contraseña actual (predeterminada), **ddguser**; a continuación, ingrese una contraseña exclusiva, vuelva a ingresar la contraseña exclusiva y seleccione **Aceptar**.

   Las contraseñas deben incluir lo siguiente:

   - Al menos ocho caracteres
   - Al menos una letra mayúscula
   - Al menos un dígito
   - Al menos un carácter especial

8 Repita el paso anterior para las cuentas *ddgconsole* y *ddgsupport*.

NOTA:
Para mantener la contraseña predeterminada, la cual es igual al nombre, haga clic en **Cancelar**. Para modificar la contraseña, ingrese **ddgconsole** o **ddgsupport** en el campo Contraseña actual.

9 En el diálogo *Configurar nombre de host*, use la tecla de retroceso para borrar el nombre de host predeterminado. Ingrese un nombre de host FQDN y seleccione **Aceptar**.

10 Si tiene varios nodos y un equilibrador de carga, ingrese un nombre de host de equilibrador de carga.

11 En el cuadro de diálogo *Configurar valores de red,* elija una de las opciones siguientes y seleccione **Aceptar**.

- (Por defecto) Usar DHCP
- (Recomendado) en el campo Usar DHCP, pulse la barra espaciadora para extraer la X e ingrese manualmente estas direcciones, según corresponda: Puerta de enlace predeterminada de la máscara de red IP estática Servidor DNS 1 Servidor DNS 2 Servidor DNS 3

NOTA:
Si usa una IP estática, también deberá crear una entrada de host en el servidor DNS.

12 Cuando aparezca la pantalla SCP, no haga clic en Aceptar. Primero debe agregar los archivos .cer y .key a la aplicación o extraerla del archivo .pfx o .p7b de CA. Consulte Utilizar la herramienta WinSCP.

NOTA:
Si hace clic en Aceptar en la pantalla de SCP antes de extraerlos, debe reiniciar Data-Guardian-Web e ir al diálogo *Configurar los valores de red*.

Uso de la herramienta WinSCP

En Windows, utilice la cuenta ddgconsole para SCP, el archivo de certificado SSL y el archivo clave SSL.

1 En Windows, abra la herramienta WinSCP.

2 En la página WinSCP, ingrese el nombre de host.

3 Ingrese el nombre de usuario por defecto ddgconsole y la contraseña por defecto (o su nombre de usuario y contraseña modificados).

4 Haga clic en **Inicio de sesión**.

5 Arrastre el certificado y la clave, además del archivo .pfx o .p7b desde su disco local al directorio **opt/dell/files**.

6 Si agregó un archivo .pfx o .p7b, ingrese una contraseña cuando se lo solicite. El certificado y la clave se extraen de la CA y se agregan a **apache2/ssl/folder**.

De manera opcional, en lugar de arrastrar el archivo .pfx o .p7b, puede extraer manualmente el certificado. A continuación se muestra un código de ejemplo:

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

A continuación, se presenta un código de ejemplo para extraer la clave privada del archivo .pfx:

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

7 Vuelva a la pantalla SCP de la Consola de administración.

Consola de administración

En la pantalla SCP de la Consola de administración:

1 Haga clic en **Aceptar**. Se abre la pantalla *Instalación del Certificado Proxy Reverso Apache2* y se muestra el certificado.

2 Seleccione un certificado y haga clic en **Entrar**.

3 Realice una de estas opciones:

- Si agregó una clave en la herramienta WinSCP, seleccione la clave en siguiente pantalla y haga clic en **Entrar**.
- Si ingresó una contraseña en la herramienta WinSCP para un archivo .pfx o .p7b, ingrese la contraseña cuando se le solicite y haga clic en **Aceptar**.

4 En la pantalla Establecer Dell Server, ingrese el nombre de host del servidor y haga clic en **Aceptar**. Aparece un cuadro de diálogo, en que se muestra una URL que se debe utilizar en el momento del aprovisionamiento. La URL se encuentra en este formato: **https://node.domain.com/edap-admin-ui/provision_node**.

> **NOTA:**
> **node.domain.com** es el nombre que introdujo en *Configurar nombre de host*. La URL señala ese nodo.

5 Abra un navegador y escriba esa URL.

6 Cuando se abra la página de aprovisionamiento de nodos de Dell Data Guardian, haga clic en **Iniciar aprovisionamiento de nodos**.

7 En la página de inicio de sesión, ingrese su correo electrónico de dominio y contraseña, y haga clic en **Iniciar sesión**. El cuadro de diálogo Dell Data Guardian indica que el aprovisionamiento fue correcto.

8 Vuelva a la pantalla de la Consola de administración que muestra la URL y haga clic en **Aceptar**. El servidor de la aplicación se reinicia y se abre Consola de administración > Menú principal.

Tareas adicionales:

- Proporcionar la URL a usuarios internos para permitirles acceder al cliente web Data Guardian.
  - Para un solo nodo, la URL se encuentra en este formato: **https://nodename/** donde el nombre de nodo refleja el nombre de host ingresado en la pantalla *Configurar nombre de host*.
  - Para varios nodos, la URL se encuentra en este formato: **https://loadBalancerName/** donde el nombre de nodo refleja el nombre de host de equilibrador de carga ingresado en la pantalla *Configurar nombre de host*.
- Para acceder al servidor en el futuro para ver las actualizaciones para esta VM o para comprobar los registros, debe habilitar SSH para esta VM. Seleccione **Configuración básica > Configuración de SSH** para habilitar SSH para un usuario ddgsupport.
- En Remote Management Console, si modifica cualquiera de las políticas de portal web basadas en nodo, debe reiniciar el VHD. Consulte Reiniciar el VHD. Después del reinicio, debe iniciar sesión con sus credenciales ddguser.

Abrir Remote Management Console

Abra Remote Management Console en esta dirección:

https://server.domain.com:8443/webui/

Las credenciales predeterminadas son **superadmin/changeit.**

Los siguientes navegadores web son compatibles con Remote Management Console:

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

Terminal de Data Guardian: Tareas de configuración básicas

Las tareas de configuración básica se pueden iniciar desde el menú principal.

Cambiar el nombre de host

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar .

1 En el menú *Configuración básica*, seleccione **Nombre de host**.

2 Use la tecla de retroceso para borrar el nombre de host de Data-Guardian-Web existente y, a continuación, ingrese el nuevo nombre de host y seleccione **Aceptar**.

Cambiar la configuración de red

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar .

1 En el menú *Configuración básica*, seleccione **Red**.
2 En la pantalla *Configurar valores de red*, elija una de las opciones siguientes y seleccione **Aceptar**.
   - (Predeterminado) Usar DHCP.
   - (Recomendado) En el campo “Usar DHCP”, presione la barra espaciadora para borrar la X e indicar manualmente estas direcciones según corresponda:

     IP estática

     Máscara de red

     Puerta de enlace predeterminada

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

   NOTA:
   Si usa una IP estática, deberá crear una entrada de host en el servidor DNS.

Cambiar contraseñas de usuario

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar .

Puede cambiar las contraseñas de los usuarios siguientes:

- ddguser (Administrador de terminal de Data Guardian): este usuario tiene acceso al Terminal de Data Guardian y a sus menús.
- ddgconsole (acceso a shell en Data Guardian): este usuario tiene acceso a shell en Data Guardian. El acceso a Shell está disponible para que el administrador de red compruebe y lleve a cabo soluciones de problemas en la red.
- ddgsupport (Administrador de Dell ProSupport): este usuario existe solo para el uso de Dell ProSupport. Por motivos de seguridad, es usted el que controla la contraseña de esta cuenta.

1 En el menú *Configuración básica*, seleccione **Cambiar contraseñas de usuario**.
2 En la pantalla *Cambiar contraseñas de usuario*, seleccione la contraseña de usuario que desee cambiar y presione **Intro**.
3 En la pantalla *Establecer contraseña,* ingrese la contraseña actual y la contraseña nueva, vuelva a ingresar la contraseña nueva y seleccione **Aceptar**.

   Las contraseñas deben incluir lo siguiente:

   - Al menos ocho caracteres
   - Al menos una letra mayúscula
   - Al menos un dígito
   - Al menos 1 carácter especial

   NOTA: Para seleccionar diferentes cuentas de usuario, utilice la barra espaciadora en el teclado para mostrar la lista de selección.

Habilitar SSH

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar .

Puede habilitar SSH para el inicio de sesión en Support Administrator, el acceso a Shell en Data Guardian y la interfaz de línea de comandos de terminal de Data Guardian.

1 En el menú *Configuración básica*, seleccione **SSH**.
2 Resalte el usuario para el que desea habilitar SSH, presione la barra espaciadora para ingresar una **X** en su campo, y seleccione **Aceptar**.

Iniciar detener servicios

Realice esta tarea solo si es necesario.

1 Para iniciar o detener todos los servicios de forma simultánea, en el menú *Configuración básica*, seleccione **Iniciar aplicación** o **Detener aplicación**.
2 En la solicitud de confirmación, seleccione **Sí**.

NOTA: Los cambios de estado de los servidores pueden tomar hasta dos minutos para completarse.

Reiniciar el VHD

Realice esta tarea solo si es necesario.

1 En el menú *Configuración básica*, seleccione **Reiniciar appliance**.
2 En la solicitud de confirmación, seleccione **Sí**.
3 Después del reinicio, inicie sesión en Data Guardian.

Apagar el VHD

Realice esta tarea solo si es necesario.

1 En el menú *Configuración básica*, desplácese hasta abajo y seleccione **Apagar appliance**.
2 En la solicitud de confirmación, seleccione **Sí**.
3 Después del reinicio, inicie sesión en Data Guardian.

Tareas del administrador

Establecer o cambiar el idioma del terminal

Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

1 En el menú principal, seleccione **Establecer idioma**.
2 Use las flechas del teclado para seleccionar el idioma deseado.

Generar un registro de instantáneas del sistema

Para generar un registro de instantánea de sistema para Dell ProSupport, seleccione en el menú principal **Herramientas de soporte.**

1 En el menú *Herramientas de soporte*, seleccione **Generar registro de instantáneas del sistema**.
2 Cuando se confirme la creación del archivo, seleccione **Aceptar**.