Dell Security Management Server Virtual

Guía de instalación e inicio rápido v10.2.5

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.

2019 - 06

Rev. A01

Contenido

1

Guía de inicio rápido

Esta Guía de inicio rápido está dirigida a usuarios con más experiencia para que puedan poner en funcionamiento Dell Server en poco tiempo. Como regla general, Dell recomienda instalar primero Dell Server, y luego realizar la instalación de los clientes.

Si desea obtener instrucciones más detalladas, consulte la Guía de instalación de Security Management Server Virtual.

Para obtener información acerca de los requisitos de Dell Server, consulte Requisitos de Security Management Server Virtual, Requisitos de la consola de administración y Requisitos del modo proxy.

Para obtener información sobre cómo actualizar un Dell Server existente, consulte Actualizar Security Management Server Virtual.

Ha finalizado la instalación

1 Diríjase al directorio en el que se almacenan los archivos de Dell Data Security y haga doble clic para importarlos en VMware Servidor virtual de administración de seguridad **v10.x.x Build x.ova**.

> **NOTA: OVA ahora cuenta con la firma SHA256 y no se importará en el cliente pesado de VMWare. Para obtener más información, consulte https://kb.vmware.com/s/article/2151537 .**

2 Encienda Security Management Server Virtual

3 Siga las instrucciones que se muestran en pantalla.

Configuración

Antes de activar usuarios, se recomienda que complete las siguientes tareas de configuración en el terminal de Servidor virtual de administración de seguridad:

- Configurar valores de SMTP
- Importar un certificado existente o registrar un certificado de servidor nuevo
- Actualizar Security Management Server Virtual
- Instalación de un cliente FTP compatible con SFTP en el puerto 22 y Configuración de usuarios de Transferencia de archivos (FTP).

  Si su organización cuenta con dispositivos externos, consulte Instalar y configurar el modo de proxy.

Apertura de la consola de administración

Abra la consola de administración en esta dirección: https://server.domain.com:8443/webui/

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

Para ver una lista de los navegadores web compatibles, consulte Requisitos de la consola de administración.

Tareas administrativas

Si aún no ha iniciado la consola de administración, hágalo ahora. Las credenciales predeterminadas son **superadmin/changeit.**

Dell le recomienda asignar funciones de administrador tan pronto como sea posible. Para realizar esta tarea ahora, consulte Asignar rol de administrador Dell.

Haga clic en "?" en la esquina superior derecha de la consola de administración para iniciar *AdminHelp*. Aparecerá la página *Introducción*. Haga clic en **Agregar dominios**.

Se establecieron las políticas de base de su organización, pero se deben modificar de acuerdo con sus necesidades específicas, como se indica a continuación (las licencias y los derechos rigen todas las activaciones):

- El cifrado basado en políticas se habilitará con el cifrado de clave común
- Se cifran los equipos que tienen unidades de cifrado automático
- No se habilita la administración de BitLocker
- No se habilita Advanced Threat Prevention
- La protección contra amenazas está deshabilitada
- No se cifran los soportes externos
- El control de puerto no administrará los puertos
- Los dispositivos con cifrado completo de disco instalado no se cifrarán
- Data Guardian está deshabilitado

Consulte el tema *Administrar políticas* de la AdminHelp para navegar hasta los Grupos de tecnología y las descripciones de las políticas.

Las tareas de la guía de inicio rápido han finalizado.

2

Guía detallada de instalación

Esta Guía de instalación está dirigida a usuarios con menos experiencia, para instalar y configurar Servidor virtual de administración de seguridad. Como regla general, Dell recomienda instalar primero Servidor virtual de administración de seguridad y, a continuación, realizar la instalación de los clientes.

Para obtener información sobre cómo actualizar un Servidor virtual de administración de seguridad existente, consulte Actualizar Security Management Server Virtual.

Acerca de Servidor virtual de administración de seguridad

La consola de administración permite que los administradores supervisen el estado de los puntos de conexión, el cumplimiento de las políticas y la protección en toda la empresa. El modo proxy proporciona una opción de modo DMZ de front-end para utilizarla con Servidor virtual de administración de seguridad.

Servidor virtual de administración de seguridad tiene las siguientes características:

- Administración centralizada de hasta 3.500 dispositivos
- Creación y administración de políticas de seguridad basadas en roles
- Recuperación de dispositivos asistida por el administrador
- Separación de tareas administrativas
- Distribución automática de políticas de seguridad
- Rutas de confianza para comunicación entre los componentes
- Generación de claves únicas de cifrado y depósito automático de claves seguras
- Auditoría y elaboración de informes de cumplimiento centralizados
- Generación automática de certificados autofirmados

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.

Requisitos

Servidor virtual de administración de seguridad

Hardware

El espacio en disco recomendado para Servidor virtual de administración de seguridad es 80 GB.

Entorno virtualizado

Servidor virtual de administración de seguridad v10.2.5 se validó para los siguientes entornos virtuales.

Dell actualmente admite alojar los servidores Dell Security Management Server o Dell Security Management Server Virtual dentro de un ambiente de infraestructura como servicio (IaaS) alojado en la nube, como los servicios web de Amazon, Azure y varios otros proveedores. La compatibilidad para estos ambientes solo se limita a la funcionalidad del servidor de aplicaciones alojado en estas máquinas virtuales, el administrador de la solución IaaS se encargará de la administración y la seguridad de estas máquinas virtuales.

Los requisitos de infraestructura adicionales (Active Directory, así como SQL Server para Dell Security Management Server) siguen siendo necesarios para que el funcionamiento sea correcto.

Entornos virtualizados

- VMware Workstation 12.5
  - CPU de 64 bits, necesario
  - Se requieren 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - Equipo host con un mínimo de dos núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- VMware Workstation 14.0
  - CPU de 64 bits, necesario
  - Se requieren 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - Equipo host con un mínimo de dos núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- VMWare Workstation 14.1
  - CPU de 64 bits, necesario
  - Se requieren 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - Equipo host con un mínimo de dos núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- VMware ESXi 6.5
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - Se requiere un mínimo de 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos del host admitidos

Entornos virtualizados

- El hardware debe cumplir con los requisitos mínimos de VMWare
- Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- VMWare ESXi 6.0
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - Se requiere un mínimo de 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos del host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- VMWare ESXi 5.5
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - Se requiere un mínimo de 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obtener una lista completa de los sistemas operativos del host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - Para obtener más información, consulte https://kb.vmware.com/s/article/1003746.

- Hyper-V Server (instalación completa o básica)
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - Se requiere un mínimo de 8 GB de RAM
  - Espacio de unidad de disco duro de 80 GB
  - No es obligatorio contar con un sistema operativo
  - Hardware que cumpla con los requisitos mínimos de Hyper-V
  - Debe ejecutarse como una máquina virtual de generación 1

NOTA: Para obtener información sobre cómo configurar Hyper-V, siga las instrucciones para sistemas operativos de terminal: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v o para sistemas operativos de servidor: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Consola de administración

Navegadores de Internet

NOTA:
El navegador debe aceptar cookies.

La siguiente tabla muestra los navegadores de Internet admitidos.

Navegadores de Internet

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

Modo proxy

Hardware

En la siguiente tabla se indican los requisitos *mínimos* de hardware:

Procesador

CPU moderna de doble núcleo (1,5 Ghz +)

RAM

RAM mínima dedicada de 2 GB/se recomienda una RAM dedicada de 4 GB

Espacio libre en disco

1,5 GB de espacio de disco libre (más el espacio de paginación virtual)

Tarjeta de red

Tarjeta de interfaz de red de 10/100/1000

Varios

Compatible con IPv4, IPv6 o una combinación de IPv4 e IPv6

Software

En la siguiente tabla se indica el software que debe estar instalado antes de instalar el servidor de modo proxy.

Requisitos previos
• **Windows Installer 4.0 o posterior** Windows Installer 4.0 o posterior debe estar instalado en el servidor en el que se vaya a hacer la instalación.
• **Paquete redistribuible de Microsoft Visual C++ 2010** Si falta este componente, el instalador lo agregará a la instalación en el sistema.
• **Microsoft .NET Framework versión 4.5.2** Microsoft ha publicado actualizaciones de seguridad para .NET Framework versión 4.5.2

NOTA:

El control de cuenta universal (UAC) debe estar deshabilitado cuando se instala en un directorio protegido. Una vez que UAC esté deshabilitado, el servidor debe reiniciarse para que el cambio tenga efecto.

Ubicación de servidores Windows en el Registro: HKLM\SOFTWARE\Dell.

En la siguiente tabla se indican los requisitos de software del servidor de modo proxy.

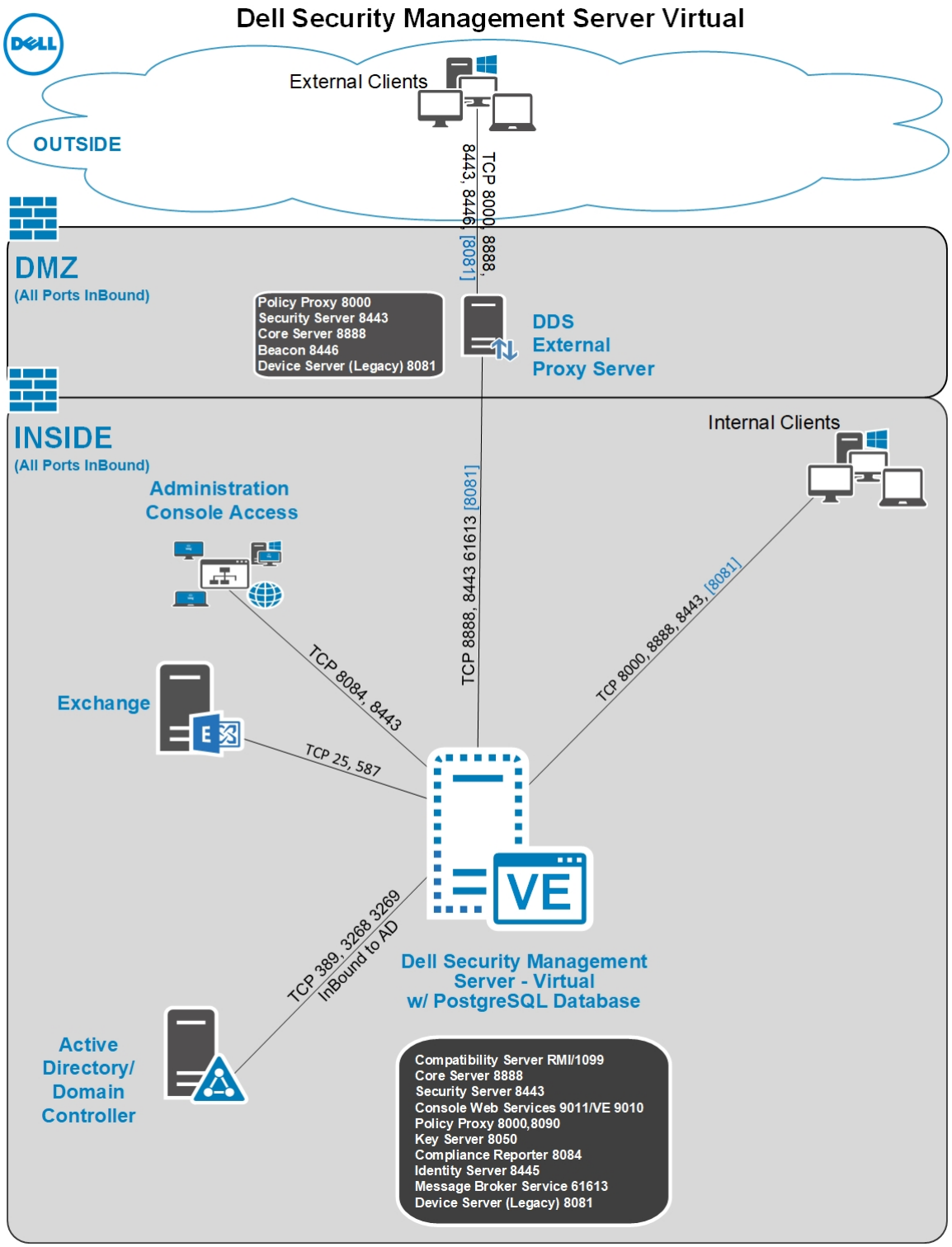
Sistema operativo
• **Windows Server 2019** - Standard Edition - Datacenter Edition • **Windows Server 2016** - Standard Edition - Datacenter Edition • **Windows Server 2012 R2** - Standard Edition - Datacenter Edition • **Repositorio LDAP** - Active Directory 2008 R2 - Active Directory 2012 R2 - Active Directory 2016

Diseño de arquitectura de Security Management Server Virtual

Las soluciones Dell Encryption, Endpoint Security Suite Enterprise y Data Guardian son productos altamente escalables según la cantidad de terminales destinados para el cifrado en su organización.

Componentes de la arquitectura

A continuación, se presenta una implementación básica para Dell Security Management Server Virtual.



Descarga e instalación del archivo OVA

En la instalación inicial, Servidor virtual de administración de seguridad se entrega como un archivo OVA, una Aplicación virtual abierta utilizada para entregar software que se ejecuta en una máquina virtual. El archivo OVA está disponible en www.dell.com/support, en las páginas de asistencia de productos de los siguientes productos de Dell Data Security:

- Cifrado

- Endpoint Security Suite Enterprise
- Data Guardian

Para descargar el archivo OVA:

1 Diríjase a la página *Controladores y descargas* del producto correspondiente mencionado anteriormente.
2 Haga clic en **Controladors y descargas.**
3 Seleccione la versión adecuada de VMware ESXi.
4 Descargue el paquete correspondiente.

Para instalar el archivo OVA:

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

1 En los medios de instalación de Dell, ubique *Security Management Server Virtual v9.x.x Build x.ova* y haga doble clic para importarlo en VMware.

> **NOTA: Si utiliza Hyper-V en vez de VMware, siga las instrucciones de Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. En el caso de los sistemas operativos basados en servidor, siga las instrucciones: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server. Si utiliza ESXi en vez de VMware, siga las instrucciones:https://kb.vmware.com/s/article/2109708 .**

2 Siga las instrucciones que se muestran en pantalla.

> **NOTA: Si se produce un error en la importación cuando se utiliza VMWare, entonces el cliente web es la ruta sugerida para importar el archivo OVA. Para obtener más información, consulte https://kb.vmware.com/s/article/2151537.**

3 Encienda Servidor virtual de administración de seguridad.
4 Seleccione el idioma para el contrato de licencia y, a continuación, seleccione **Mostrar CLUF**.
5 Lea el contrato y seleccione **Aceptar CLUF**.
6 Si hay una actualización disponible, seleccione **Aceptar**.
7 Seleccione **Modo conectado** o **Modo desconectado**.

> **NOTA:**
> Si selecciona **Modo desconectado**, no se podrá cambiar nunca al modo conectado.
>
> El modo desconectado aísla Dell Server desde Internet, de una LAN no protegida o de otras redes no protegidas. Todas las actualizaciones deben realizarse manualmente. Para obtener más información con respecto a las políticas y el modo desconectado, consulte *AdminHelp*.

8 En *Establecer contraseña de delluser*, ingrese la contraseña actual (predeterminada), **delluser**, luego ingrese una contraseña única, vuelva a ingresar esa contraseña y seleccione **Aplicar**.

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: Se puede conservar la contraseña predeterminada mediante la selección de Cancelar o si se presiona Escape en el teclado.**

9 Seleccione **Cerrar** para acceder a la ventana de configuración del nombre de host.
10 En *Configurar nombre de host*, utilice la tecla de retroceso para quitar el nombre de host predeterminado. Ingrese un nombre de host exclusivo y seleccione **Aceptar**.

11 En *Configurar ajustes de red*, escoja cualquiera de las siguientes opciones y seleccione **Aceptar**.

- (Predeterminado) Utilizar DHCP (IPv4)
- (Recomendado) En *Utilizar DHCP*, presione la barra espaciadora para quitar la X e ingresar manualmente estas direcciones, según corresponda:

  IP estática

  Máscara de red

  Puerta de enlace predeterminada

  Servidor DNS 1

  Servidor DNS 2

  Servidor DNS 3

  Se puede seleccionar IPv6 o IPv4 para una configuración estática.
- **NOTA: Si usa una IP estática, también deberá crear una entrada de host en el servidor DNS.**

12 En la solicitud de confirmación de zona horaria, seleccione **Aceptar**.

13 Cuando se muestre el mensaje en el que se indica que se completó la configuración de arranque inicial, seleccione **Aceptar**.

14 Configurar valores de SMTP.

15 Importar un certificado existente o registrar un certificado de servidor nuevo.

16 Actualizar Security Management Server Virtual.

17 Instalación de un cliente FTP compatible con SFTP en el puerto 22 y Configuración de usuarios de Transferencia de archivos (FTP).

Las tareas de instalación de Servidor virtual de administración de seguridad están completas.

Apertura de la consola de administración

Abra la consola de administración en esta dirección: https://server.domain.com:8443/webui/

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

Para ver una lista de los navegadores web compatibles, consulte Requisitos de la consola de administración.

Instalación y configuración del modo de proxy

El modo proxy proporciona una opción de front-end (modo DMZ) para utilizarla con Dell Server. Si desea implementar componentes Dell en la DMZ, asegúrese de que estén protegidos apropiadamente frente a ataques.

NOTA: El servicio Beacon se instala como parte de esta instalación para ser compatible con el aviso de devolución de llamada de Data Guardian, que inserta un aviso de devolución de llamada en cada archivo protegido por Data Guardian cuando se permiten o aplican documentos protegidos de Office dentro del entorno. Esto permite la comunicación de cualquier dispositivo, en cualquier ubicación, con el servidor de front-end. Asegúrese de que se ha configurado la seguridad de la red necesaria antes de utilizar el aviso de devolución de llamada.

Para llevar a cabo esta instalación, debe contar con el nombre completo del host del servidor DMZ.

1 En el medio de instalación de Dell, navegue hasta el directorio de Servidor de administración de seguridad. **Descomprima** (NO copie/pegue ni arrastre/suelte) Servidor de administración de seguridad-x64 en el directorio raíz del servidor en el que vaya a instalar Servidor virtual de administración de seguridad. ***Si copia/pega o arrastra/suelta elementos, se generarán errores y no se llevará a cabo la instalación correctamente.***

2 Haga doble clic en **setup.exe**.

3 Seleccione el idioma para la instalación y haga clic en **Aceptar**.

4 Si aún no se han instalado los requisitos previos, aparecerá un mensaje que le informará sobre qué requisitos serán instalados. Haga clic en **Instalar**.

5 Haga clic en **Siguiente** en el cuadro de diálogo de bienvenida.

6 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.

7 Ingrese la clave de producto de 32 caracteres y haga clic en **Siguiente**. La clave de producto se encuentra en el archivo EnterpriseServerInstallKey.ini.

8 Seleccione **Instalación de front-end** y haga clic en **Siguiente**.

9 Para instalar el servidor de front-end en la ubicación predeterminada de C:\Program Files\Dell, haga clic en **Siguiente**. De lo contrario, haga clic en **Cambiar** para seleccionar otra ubicación y, a continuación, haga clic en **Siguiente**.

10 Tiene la opción de escoger los tipos de certificados digitales que se utilizarán.

> **NOTA: Se recomienda encarecidamente que se utilice el certificado digital de una autoridad de certificación de confianza.**

Seleccione la opción "a" o "b" a continuación:

a Para utilizar un certificado existente que haya adquirido de una entidad emisora de certificados, seleccione **Importar un certificado existente** y haga clic en **Siguiente**.

b Para crear un certificado autofirmado, seleccione **Crear un certificado autofirmado e importarlo en un almacenamiento de claves y haga clic en Siguiente.**

En el cuadro de diálogo *Crear certificado autofirmado*, ingrese la siguiente información:

Nombre de equipo completo (ejemplo: nombreequipo.dominio.com)

Organización

Unidad organizacional (ejemplo: Seguridad)

Ciudad

Estado (nombre completo)

País: abreviación de país de dos letras

Haga clic en **Siguiente**.

> **NOTA: El certificado vence dentro de 10 años, de manera predeterminada.**

11 En el cuadro de diálogo *Configuración del servidor de front-end*, ingrese el nombre completo del host o el alias de DNS del servidor de back-end, seleccione **Dell Security Management Server** y haga clic en **Siguiente**.

12 Desde el cuadro de diálogo *Configuración de la instalación del servidor front-end*, puede ver o editar nombres de host y puertos.

- Para aceptar los nombres de host y puertos predeterminados, en el cuadro de diálogo *Configuración de la instalación del servidor front-end*, haga clic en **Siguiente**.
- Para ver o editar nombres de host, en el cuadro de diálogo *Configuración del servidor front-end*, haga clic en **Editar nombres de host**. Edite nombres de host solo si fuera necesario. Dell recomienda utilizar los valores predeterminados.

> **NOTA:**
> Un nombre de host no puede contener un guion bajo ("_").

Desmarque un proxy solo si está seguro de que no desea configurarlo para la instalación. Si desmarca un proxy en este cuadro de diálogo, no se instalará.

Cuando termine, haga clic en **Aceptar**.

- Para ver o editar puertos, en el cuadro de diálogo *Configuración del servidor front-end*, haga clic en **Editar puertos externos** o **Editar puertos de conexión internos**. Edite puertos solo si fuera necesario. Dell recomienda utilizar los valores predeterminados.

Si deseleccionara un proxy en el cuadro de diálogo *Editar nombres de host front-end*, su puerto no se muestra en los cuadros de diálogo Puertos externos ni Puertos internos.

Cuando termine, haga clic en **Aceptar**.

13 En el cuadro de diálogo *Preparado para instalar el programa*, haga clic en **Instalar**.

14 Cuando se complete la instalación, haga clic en **Finalizar**.

Tareas básicas de configuración del terminal de

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

Comprobar el panel de sistema

Para comprobar el estado de los servicios de Dell Server, en el menú principal, seleccione **Panel de sistema**.

En el widget *Información del sistema* se muestra la versión actual, el nombre de host, la dirección IP y el uso de la CPU, la memoria y el disco.

En el widget *Historial de versión* se muestran los cambios de schema de la base de datos con versión. Los datos provienen de la tabla "información" y están ordenados por hora y la versión más reciente se encuentra en la parte superior.

En la siguiente tabla se explican todos los servicios y sus funciones en el widget *Estado del servicio*.

Nombre	Descripción
Message Broker	Bus de Enterprise Server
Identity Server	Procesa las solicitudes de autenticación de dominios.
Compatibility Server	Un servicio para administrar la arquitectura empresarial.
Security Server	Proporciona un mecanismo para controlar comandos y comunicaciones con Active Directory.
Compliance Reporter	Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías.
Core Server	Un servicio para administrar la arquitectura empresarial. Este servicio también controla toda la activación, política y recopilación de inventario desde los dispositivos basados en "agentes".
Core Server HA (Alta disponibilidad)	Un servicio de alta disponibilidad que permite una seguridad aumentada y rendimiento de conexiones HTTPS al administrar la arquitectura empresarial.
Inventory Server	Procesa la cola de inventario.
Forensic Server	Proporciona servicios web para la API forense.
Policy Proxy	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario.

Si es necesario, los servicios se supervisan y reinician automáticamente.

NOTA: Si el proceso Databasecustomizer falla, los servidores pasan al estado “Error de ejecución”. Para ver el registro de Databasecustomizer, seleccione “Ver registros” en el menú principal.

Cambiar el nombre de host

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

1 En el menú *Configuración básica*, seleccione **Nombre de host**.
2 Utilice la tecla de retroceso para eliminar el nombre de host existente de y reemplazarlo con un nuevo nombre de host; luego, seleccione **Aceptar**.

Cambiar la configuración de red

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

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) Utilizar DHCP (IPv4).
   - (Recomendado) En *Utilizar DHCP*, presione la barra espaciadora para eliminar la X e ingresar manualmente estas direcciones según corresponda:

     IP estática

     Máscara de red

     Puerta de enlace predeterminada

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

     Se puede seleccionar IPv6 o IPv4 para una configuración estática.

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

Establecer la compatibilidad del servidor DMZ

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

1 En el menú *Configuración básica*, seleccione **Soporte para servidor DMZ**.
2 Utilice la barra espaciadora para ingresar una **X** en el campo Habilitar asistencia de servidor DMZ
3 Ingrese el nombre de dominio completo del servidor DMZ y seleccione **Aceptar**.

NOTA: Para aprovechar un servidor DMZ, consulte las instrucciones de instalación de un servidor proxy que se indican en Instalación y configuración del modo proxy.

Cambiar la zona horaria

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

1 En el menú *Configuración básica*, seleccione **Zona horaria.**
2 En la pantalla *Zona horaria*, utilice las flechas del teclado para resaltar su zona horaria y seleccione **Intro**.

Actualizar Servidor virtual de administración de seguridad

Para obtener información acerca de una actualización en específico, consulte la *asesoría técnica de Servidor virtual de administración de seguridad*, que se ubica en dell.com/support. Para ver la versión y fecha de instalación de una actualización que ya está aplicada, revise el *Panel de sistema*.

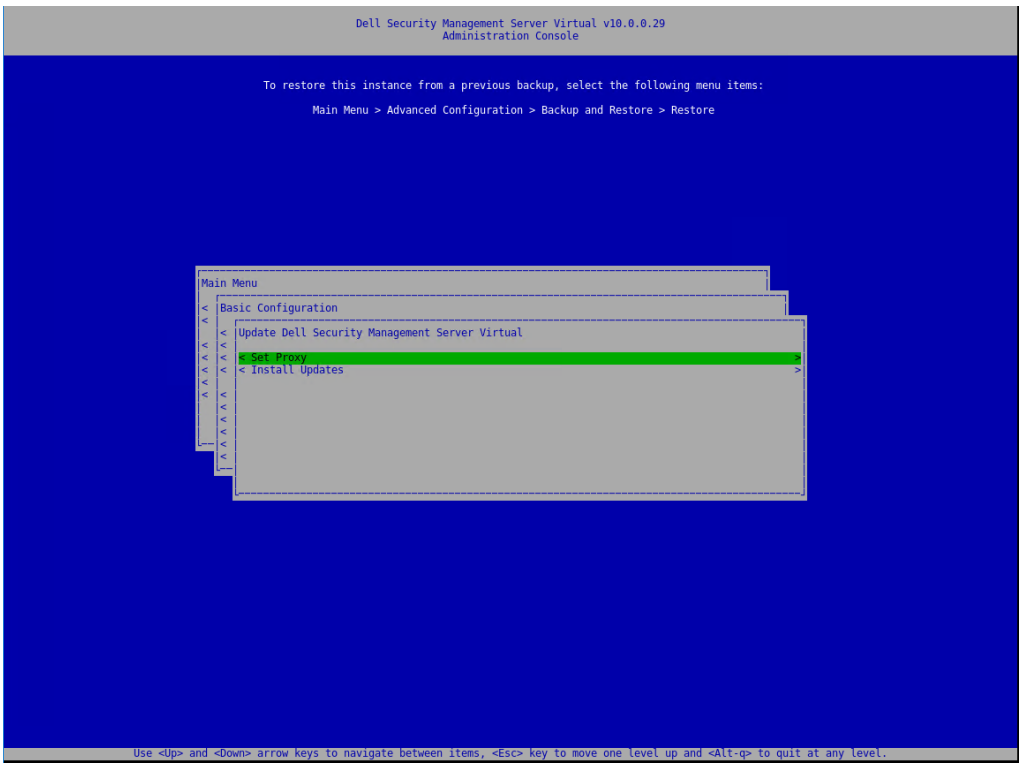
Para recibir notificaciones de correo electrónico cuando estén disponibles las actualizaciones de Dell Server, consulte Configurar valores de SMTP.

Si se han realizado cambios en las políticas, pero no se han confirmado en la consola de administración, confirme tales cambios antes de actualizar Dell Server:

1 Como un administrador de Dell, inicie sesión en la Management Console.
2 En el menú izquierdo, haga clic en **Administración** > **Confirmar**.
3 Ingrese una descripción del cambio en el campo Comentario.
4 Haga clic en **Confirmar políticas**.
5 Cuando haya realizado la confirmación, cierre la sesión de la consola de administración.

Actualizar Servidor virtual de administración de seguridad (Modo conectado)

1 Dell recomienda realizar una copia de seguridad periódicamente. Antes de actualizar, asegúrese de que el proceso de copia de seguridad ha estado funcionando correctamente. Consulte Realizar copias de seguridad y restaurar.
2 En el menú **Configuración básica**, seleccione **Actualizar Dell Security Management Server Virtual**.



NOTA: Es posible que el número de la versión sea distinto del que se presenta en la captura de pantalla adjunta.

3 Seleccione la acción deseada:

- Establecer la configuración de proxy: Seleccione esta opción para establecer la configuración de proxy a fin de descargar actualizaciones.

  En la pantalla *Ajustar configuración de proxy*, presione la barra espaciadora para ingresar una **X** en *Usar proxy*. Ingrese el HTTPS y HTTP. Si se requiere una autenticación de firewall, presione la barra espaciadora para ingresar una **X** en Autenticación obligatoria. Ingrese el nombre de usuario y la contraseña, y seleccione **Aceptar**.

  NOTA: Ahora esta opción de proxy establecida actualiza la configuración de proxy para varias aplicaciones basadas en java para sacar las licencias en las cajas y, también, para la comunicación de SaaS en Endpoint Security Suite Enterprise y en la infraestructura de back-end de Dell/Credant.

- Cuando se selecciona **Instalar actualizaciones**, Security Management Server Virtual consulta los repositorios predeterminados, los repositorios de Ubuntu predeterminados y dist.ddspproduction.com, el repositorio personalizado de Dell que contiene las actualizaciones de las aplicaciones.

  NOTA: Dell consulta dist.ddspproduction.com a través del puerto 443 y el puerto 80 para todas las actualizaciones de Ubuntu. Se descargan todas las actualizaciones disponibles. La configuración de proxy definida en Configuración de proxy, se utiliza para la descarga de las conexiones de los puertos 443 y 80.

Actualizar Servidor virtual de administración de seguridad (Modo desconectado)

1 Dell recomienda realizar una copia de seguridad periódicamente. Antes de actualizar, asegúrese de que el proceso de copia de seguridad ha estado funcionando correctamente. Consulte Realizar copias de seguridad y restaurar.

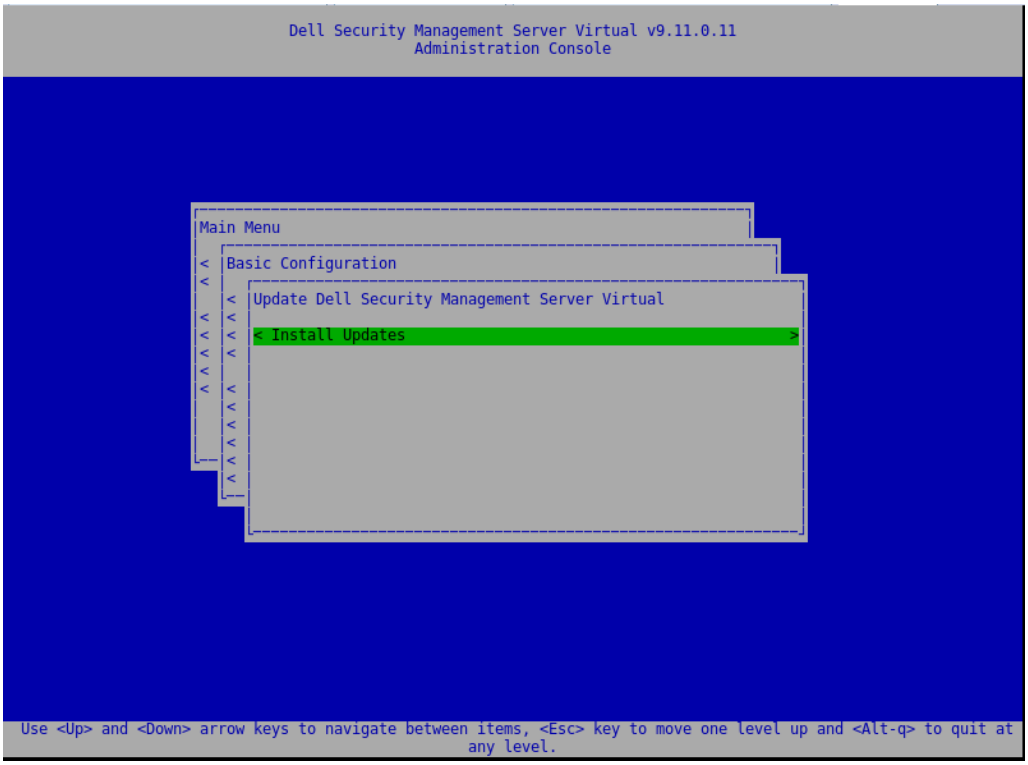
2 Obtenga el archivo .deb que contiene la última actualización de Dell Server en Dell ProSupport.

3 Almacene el archivo .deb en la carpeta /updates en el servidor FTP seguro de Dell Server.

Asegúrese de que el cliente de FTP admite SFTP en el puerto 22 y que el usuario de FTP está configurado. Consulte Configurar usuarios de Transferencia de archivos (FTP).

4 En el menú **Configuración básica**, seleccione **Actualizar Security Management Server Virtual**.

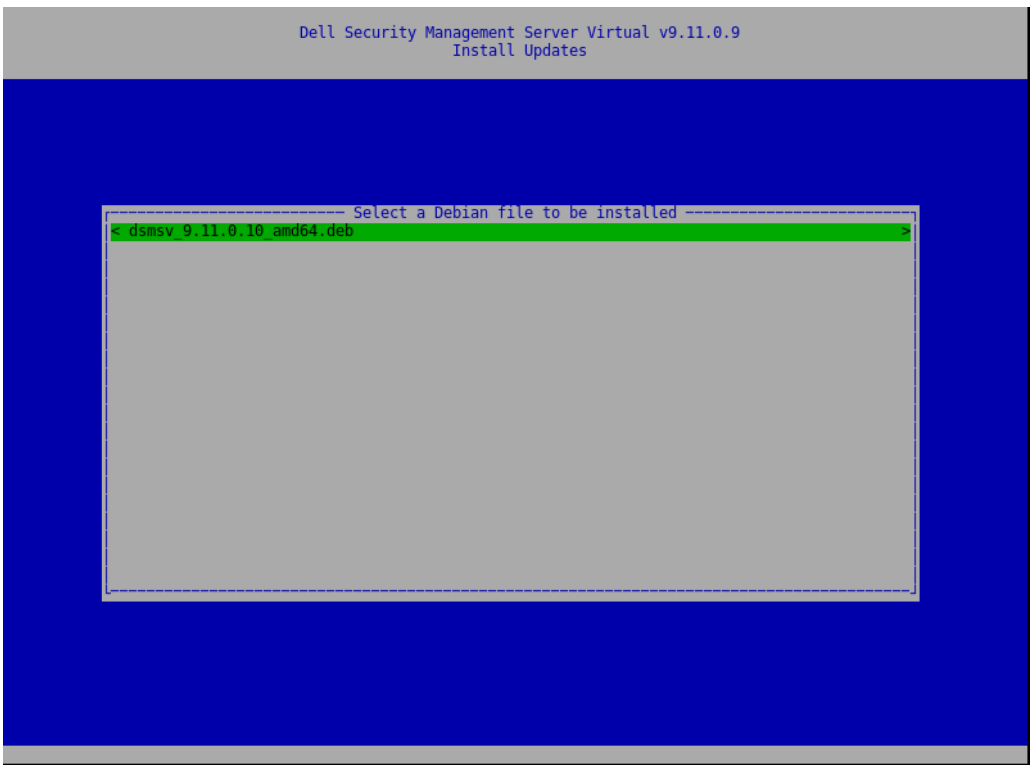
5 Seleccione **Instalar actualizaciones** y presione **Intro**.



NOTA: Es posible que el número de la versión sea distinto del que se presenta en la captura de pantalla adjunta.

Si el archivo .deb no se muestra, asegúrese de que el archivo .deb está almacenada en la ubicación adecuada.

6 Seleccione el archivo de actualización .deb archivo que desea instalar y pulse **Intro**.



NOTA: Es posible que el número de la versión sea distinto del que se presenta en la captura de pantalla adjunta.

Cambiar contraseñas de usuario

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

Puede cambiar las contraseñas de los usuarios siguientes:

- delluser (administrador de terminal): Este usuario tiene acceso al terminal de Dell Server y sus menús.
- dellconsole (acceso al shell): Este usuario tiene acceso al shell de Dell Server. El acceso a Shell está disponible para que el administrador de red compruebe y lleve a cabo soluciones de problemas en la red.
- dellsupport (administrador de Dell ProSupport): Este usuario tiene derechos "sudo" y se debe utilizar en forma moderada. 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.

Configurar usuarios de Secure File Transfer (SFTP)

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

1 En el menú *Configuración básica*, seleccione **SFTP**.

2 Para agregar a un usuario SFTP y definir una contraseña, en la pantalla *SFTP* presione **Intro** o la tecla hacia abajo en el campo de *Estado* para el usuario. Si se presiona la barra espaciadora, se puede actualizar o eliminar a un usuario existente. Para deshabilitar un usuario SFTP, seleccione **Eliminar** después de seleccionar al usuario y, a continuación, seleccione **Sí** en la pantalla de confirmación de SFTP.

3 Ingrese un nombre de usuario y una contraseña para el usuario de SFTP.

Las contraseñas deben incluir lo siguiente:

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

4 Cuando haya terminado de agregar usuarios de SFTP, seleccione **Aplicar**.

Habilitar SSH

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

Puede habilitar SSH para el inicio de sesión del administrador de asistencia, el acceso al shell y la interfaz de la línea de comandos del terminal.

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

Iniciar detener servicios

Realice esta tarea solo si es necesario.

1 Para iniciar o detener, en forma simultánea, todos los servicios, 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 Servidor virtual de administración de seguridad.

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 Servidor virtual de administración de seguridad.

Tareas avanzadas de configuración de terminal

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

Configurar la rotación de registros

NOTA: En las siguientes instrucciones, se define la rotación de registros de las aplicaciones de Dell Security Management Server Virtual que admiten la rotación de registros.

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

La rotación de registros diaria es la opción predeterminada. Para cambiar la rotación de registros predeterminada, en el menú *Configuración avanzada*, seleccione **Configuración de rotación de registros**.

Para deshabilitar la rotación de registros, utilice la barra espaciadora para ingresar una **X** en *Sin rotación* y seleccione **Aceptar**.

Para habilitar la rotación de registros, siga estos pasos:

1 Para habilitar una rotación diaria, semanal o mensual, use la barra espaciadora para ingresar una **X** en el campo correspondiente. En el caso de las rotaciones semanales, utilice el menú desplegable para seleccionar el día correspondiente de la semana. En el caso de las rotaciones mensuales, ingrese el día correspondiente del mes.
2 Ingrese la hora de la rotación en *Hora de rotación de registro*.
3 Seleccione **Aceptar**.

Realizar copias de seguridad y restaurar

Las copias de seguridad se pueden configurar o realizar en cualquier momento y no son necesarias para empezar a utilizar Servidor virtual de administración de seguridad. Dell recomienda configurar un proceso de copia de seguridad periódico. Para obtener más información, consulte http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Cuando se almacenan en Dell Server y el disco esté al 90 % de su capacidad, no se almacenarán las copias de seguridad más nuevas. Si se configuraron las notificaciones por correo electrónico, recibirá una notificación por correo electrónico en la que se indica que hay poco espacio de asignación de disco.

NOTA:
Para conservar el espacio de partición de disco e impedir la eliminación automática de los respaldos, elimine los respaldos innecesarios del almacenamiento.

Se realizan copias de seguridad diariamente de forma predeterminada. Dell recomienda que se almacenen copias de seguridad en un servidor FTP seguro externo a una frecuencia que cumpla con los requisitos de la organización para las copias de seguridad y el uso adecuado del espacio de almacenamiento.

Para configurar una programación de copia de seguridad, en el menú *Configuración avanzada*, seleccione **Copias de seguridad y restauración > Configuración** y siga estos pasos:

1 Para habilitar la creación de respaldos diarios, semanales o mensuales, utilice la barra espaciadora para ingresar una **X** en el campo correspondiente. Para copias de seguridad semanales o mensuales, indique el día de la semana o el mes como numeral, donde Lunes=1. Para deshabilitar la creación de respaldos, utilice la barra espaciadora para ingresar una **X** en *Sin respaldo* y seleccione **Aceptar**.
2 Ingrese la hora del respaldo en *Tiempo de ejecución del respaldo*.
3 Seleccione **Aceptar**.

Para realizar una copia de seguridad inmediata, en el menú *Configuración avanzada*, seleccione **Copias de seguridad y restauración > Hacer copia de seguridad ahora**. Cuando aparezca el mensaje de confirmación de copia de seguridad, seleccione **Aceptar**.

NOTA:
Antes de comenzar a realizar una operación de restauración, todos los servicios del Dell Server se deben estar ejecutando. Comprobar estado del servidor. Si no se están ejecutando todos los servicios, reinícielos. Para obtener más información, consulte Iniciar o detener servicios. Comience a restaurarlos ***solo*** cuando ***todos*** los servicios se estén ejecutando.

Para realizar una restauración a partir de un respaldo, en el menú *Configuración avanzada*, seleccione **Respaldar y restaurar > Restaurar**, y, a continuación, seleccione el archivo de respaldo que se va a restaurar. En la pantalla de confirmación, seleccione **Sí**.

El respaldo se restaura después de reiniciarlo.

Almacenar copias de seguridad en un servidor FTP seguro

Para almacenar copias de seguridad en un servidor FTP, el cliente FTP debe admitir SFTP en el puerto 22.

Según los requisitos de la copia de seguridad de la organización, las copias de seguridad se pueden descargar de las siguientes maneras:

- Manualmente
- Mediante una secuencia de comandos automatizada
- Mediante la solución de copia de seguridad aprobada de la organización

Para descargar las copias de seguridad utilizando la solución de copia de seguridad de la organización, obtenga instrucciones detalladas del proveedor de la solución de copia de seguridad.

NOTA:
Dell Server está basado en Linux Debian Ubuntu x64.

Inicie sesión en Dell Server como dellsupport y utilice el comando `sudo` para configurar la solución de copia de seguridad:

`sudo` <instrucciones del proveedor de la solución de copia de seguridad>

Contenido de copia de seguridad de las siguientes carpetas:

/backup (obligatorio)

/certificates (muy recomendado)

/support (opcional)

Cuando se complete el proceso sudo, escriba **exit** y presione **Intro** hasta que se muestre la solicitud de inicio de sesión.

Configurar valores de SMTP

Para recibir notificaciones por correo electrónico de Data Guardian, **o** para utilizarlo, siga los pasos que se indican en esta sección para configurar los ajustes de SMTP. Las notificaciones por correo electrónico permiten informarles a los destinatarios acerca de los estados de error del estado de Dell Server, las actualizaciones de contraseña, la disponibilidad de las actualizaciones de Dell Server y los problemas de licencia de los clientes.

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

Para establecer la configuración de SMTP, siga estos pasos:

1 En el menú *Configuración avanzada*, seleccione **Notificaciones de correo electrónico**.
2 Para habilitar las alertas por correo electrónico, en la pantalla de notificaciones por correo electrónico, presione la barra espaciadora para ingresar una **X** en *Habilitar alertas por correo electrónico*.
3 Ingrese el nombre de dominio completo del servidor SMTP.
4 Ingrese el puerto SMTP.
5 Ingrese el usuario SMTP
6 Ingresar la contraseña de SMTP
7 En el campo *Enviar notificaciones desde*, ingrese el ID de cuenta del correo electrónico para enviar notificaciones por correo electrónico.
8 En el campo *Enviar el estado del servidor a*, ingrese un ID de cuenta de correo electrónico para enviar notificaciones de estado del servidor. Los destinatarios se deben separar con coma o punto y coma.
9 En el campo *Enviar cambios de contraseña a*, ingrese un ID de cuenta de correo electrónico para enviar notificaciones de cambio de contraseña.
10 En el campo *Enviar actualizaciones de software a*, ingrese un ID de cuenta de correo electrónico para enviar notificaciones de actualización de software.
11 En el campo *Recordatorio de alerta de servicio*, para activar los recordatorios, presione la barra espaciadora para ingresar una **X** y luego establezca el intervalo de recordatorio en minutos. Se desencadena un Recordatorio de alerta de servicio cuando se pasa el intervalo del recordatorio después de que una notificación se haya enviado sobre un problema de estado del sistema y el host o los servicios permanezcan en el mismo estado.

12 En el campo *Informe de resumen*, para habilitar los informes de las notificaciones, seleccione el intervalo deseado (diario, semanal o mensual) y luego presione la barra espaciadora para ingresar una **X**.

13 Seleccione **Aceptar**.

Importar un certificado existente o registrar un certificado de servidor nuevo

Por medio de Servidor virtual de administración de seguridad, puede importar un certificado existente o crear una solicitud de certificado.

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

Importar un certificado existente de servidor

1 Exporte el certificado existente y su cadena de confianza entera desde su KeyStore.

> **NOTA: Conserve la contraseña de exportación porque la necesitará cuando importe el certificado en Servidor virtual de administración de seguridad.**

2 En el servidor FTP de Dell Server, almacene el certificado en **/certificates**.

3 En el menú *Configuración avanzada*, seleccione **Certificados de servidor**.

4 Seleccione **Importar certificado existente**.

5 Seleccione un archivo de certificado para instalar en Dell Server.

6 Cuando se le solicite, ingrese la contraseña de exportación del certificado y seleccione **Aceptar**.

7 Cuando se complete el proceso de importación, seleccione **Aceptar**.

> **NOTA: Para obtener más información, consulte http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

Suscribir un nuevo certificado de servidor

1 En el menú *Configuración avanzada*, seleccione **Certificados de servidor**.

2 Seleccione **Certificado de servidor nuevo**.

3 Seleccione **Crear solicitud de certificado**.

4 Rellene los campos *Generar solicitud de certificado*:

- Código del país: código de dos letras del país.
- *Estado/provincia*: ingrese el nombre de la provincia o el estado sin abreviar (por ejemplo, Texas).
- *Nombre de la localidad/ciudad:* ingrese el valor adecuado (por ejemplo, Dallas).
- Organización: ingrese el valor correspondiente (por ejemplo, Dell).
- *Unidad organizacional:* ingrese el valor adecuado (por ejemplo, Seguridad).
- *Nombre común:* Ingrese el nombre de dominio plenamente calificado de Dell Server. Este nombre de dominio completo incluye el nombre de host y el nombre de dominio (por ejemplo: servidor.dominio.com).
- *Id. de correo electrónico:* ingrese la dirección de correo electrónico a la que se deberá enviar su CSR.

5 Siga el proceso de su organización para la adquisición de un certificado de servidor SSL de una autoridad de certificación. Envíe el contenido del archivo CSR para su firma.

6 Cuando reciba el certificado firmado, expórtelo como archivo .p7b y descargue la cadena de confianza completa en formato .der.

7 Haga copias de seguridad del certificado y la cadena de confianza.

8 Cargue el archivo del certificado y su cadena de confianza entera al servidor FTP de Dell Server.

9 En el menú *Configuración avanzada*, seleccione **Certificados de servidor**.

10 Seleccione **Certificado de servidor nuevo**.

11 Seleccione `Certificado de suscripción completado`.

12 Seleccione el archivo de certificado para instalar en Dell Server.

13 Si se le solicita, specifique la contraseña del certificado: **changeit**.

Para habilitar la validación de confianza en los clientes de cifrado basados en Windows, consulte Habilitar la verificación de cadena de confianza del administrador.

Crear e instalar un certificado autofirmado

NOTA: Los certificados autofirmados generados automáticamente se generan por 10 años.

1 En el menú *Configuración avanzada*, Dell Server, seleccione **Certificados del servidor**.

2 Seleccione **Crear e instalar certificados autofirmados**.

3 Para confirmar que desea reemplazar un certificado instalado previamente con un nuevo certificado**,** haga clic en Sí.

4 Ingrese la contraseña del certificado: **changeit**.

5 Una vez que se haya instalado el nuevo certificado, seleccione **Aceptar** y espere a que se reinicien los servicios.

Los servicios se reinician automáticamente.

Habilitación del acceso a la base de datos

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar Servidor virtual de administración de seguridad.

NOTA: Dell le recomienda habilitar el acceso a la base de datos solo cuando sea necesario y deshabilitarlo cuando ya no lo sea.

1 En el menú *Configuración avanzada*, seleccione **Acceso a la base de datos**.

2 Utilice la barra espaciadora para ingresar una **X** en *Habilitar acceso a la base de datos* y seleccione **Aceptar**. Si la contraseña de la base de datos no se ha configurado aún, se mostrará un indicador para la contraseña de la base de datos.

3 Ingrese la contraseña de la base de datos.

4 Vuelva a ingresar la contraseña de la base de datos.

Los componentes de la aplicación Dell Data Security se detienen automáticamente.

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.

Ver registros

Para comprobar los siguientes registros, en el menú principal, seleccione **Ver registros**.

- Registros del sistema
  - Registro Syslog
  - Registro Mail
  - Registro Auth (SSH)
  - Registro Postgres
  - Registro Monitor

- Registros del servidor
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- Consola de administración
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Registro Databasecustomizer

NOTA: Para navegar por esta pantalla, utilice lo siguiente:

- Para ir al final del registro, puede mantener la tecla Alt derecha presionada y, a continuación, presionar la tecla "/" en el teclado
- Para salir del registro, mantenga presionada la tecla control izquierda y pulse "x" en el teclado.
- las teclas de flecha permiten la navegación.
- las teclas re pág y av pág se desplazan hacia arriba o abajo en páginas, una a la vez.
- la barra espaciadora avanza los registros en una página.

Apertura de la interfaz de la línea de comandos

Para abrir la interfaz de la línea de comandos, en el menú principal, seleccione **Iniciar Shell**.

Para salir de la interfaz de línea de comandos, escriba **exit** y presione **Intro**.

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**.

3

Mantenimiento de

Elimine los respaldos innecesarios de Servidor virtual de administración de seguridad.

Solo se retendrán las diez copias de seguridad más recientes. Si el espacio de partición de disco está al diez por ciento o menos, no se almacenarán más copias de seguridad. Si se da esta situación, recibirá una notificación de correo electrónico en la que se indicará que el espacio de asignación del disco está en un nivel bajo.

4

Solución de problemas

Si se produce un error, y tiene notificaciones de correo electrónico configuradas, recibirá una notificación de correo electrónico. En función de lo indicado en la notificación de correo electrónico, siga estos pasos:

1 Consultar los archivos de registro correspondientes.
2 Reiniciar los servicios según sea necesario. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.
3 Generar un registro de instantáneas del sistema.
4 Ponerse en contacto con Dell ProSupport. Para obtener más información, consulte Póngase en contacto con Dell ProSupport.

5

Configuración posterior a la instalación

Después de la instalación, es posible que algunos componentes de su entorno se deban configurar en función de la solución de Dell Data Security utilizada en su organización.

Después de instalar Servidor virtual de administración de seguridad, se deben modificar los siguientes elementos predeterminados:

- Cambie la contraseña del servidor de back-end en la siguiente ubicación:

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- Cambie la contraseña de todos los servidores de front-end de su entorno en la siguiente ubicación:

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

La contraseña se muestra de la siguiente manera: `proxy-server.password=ENC(<texthere>)`

Para cambiar la contraseña:

1 Seleccione: `ENC(<texthere>)`

2 Cambie el texto seleccionado a: `CLR(<newpasswordhere>)`

Después de reiniciar el servicio, la línea modificada cambia a `ENC` de `CLR` y la contraseña se cifra.

NOTA: el proxy-server.username también se puede modificar, pero esto debe coincidir dentro del archivo application.properties de Message Broker y todos los servidores de front-end activos.

Configuración de Data Guardian

Para configurar Dell Server a fin de que sea compatible con Data Guardian, en la consola de administración, establezca una de estas políticas, o ambas, como **Activado**: *Documentos protegidos de Office* y *Cifrado en la nube*.

Para obtener instrucciones sobre cómo instalar el cliente Data Guardian, consulte la *Guía del administrador de Data Guardian* o la *Guía del usuario* de *Data Guardian*. Se recomienda a los administradores activar SMTP para permitir que Dell Data Guardian envíe correos electrónicos a usuarios externos y para permitir que la administración de claves sea más sencilla para los creadores.

Validación de la comprobación de cadenas de confianza del administrador

Si un certificado autofirmado se utiliza en Servidor virtual de administración de seguridad para SED o BitLocker Manager, la validación de confianza SSL/TLS debe permanecer ***deshabilitada*** en la computadora cliente. Antes de habilitar la validación de confianza SSL/TLS en el equipo cliente, deberán cumplirse los siguientes requisitos:

- Un certificado firmado por una autoridad raíz (como por ejemplo, Entrust o Verisign) deberá ser importado a Dell Server. Consulte Importar un certificado existente o registrar un certificado de servidor nuevo.
- La cadena completa de confianza del certificado deberá ser almacenada en el keystore de Microsoft del equipo cliente.

Para deshabilitar la validación de confianza de SSL/TLS en la computadora cliente, cambie el valor de la siguiente entrada de registro a 1:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

6

Tareas del administrador de la consola de administración

Asignar rol de administrador Dell

1 Como administrador de Security Management Server Virtual, inicie sesión en la consola de administración: https://server.domain.com:8443/webui/. Las credenciales predeterminadas son **superadmin/changeit.**

2 En el panel izquierdo, haga clic en **Poblaciones** > **Dominios**.

3 Haga clic en un dominio en el que desee agregar a un usuario.

4 En la página de Detalles del dominio, haga clic en la pestaña **Miembros**.

5 Haga clic en **Agregar usuario**.

6 Ingrese un filtro para buscar el nombre de usuario a través de nombre común, nombre principal universal o sAMAccountName. El carácter comodín es el *.

Es necesario definir un nombre común, un nombre principal universal y un sAMAccountName para cada usuario en el servidor de directorios empresarial. Si un usuario es miembro de un dominio o grupo, pero no se muestra en la lista de miembros de dominio o grupo, asegúrese de que los tres nombres estén correctamente definidos para el usuario en el servidor de directorio empresarial.

La consulta buscará automáticamente por nombre común, luego por UPN y, por último, por nombre de sAMAccount, hasta que se encuentre una coincidencia.

7 Seleccione los usuarios de la *Lista de usuarios del directorio* que se agregarán al dominio. Utilice <Mayús><clic> o <Ctrl><clic> para seleccionar varios usuarios.

8 Haga clic en **Agregar**.

9 Desde la barra del menú, haga clic sobre la pestaña **Detalles y acciones** del usuario específico.

10 Desplácese por la barra del menú y seleccione la pestaña **Admin**.

11 Seleccione las funciones administrativas que desea asignar a este usuario.

12 Haga clic en **Guardar**.

Iniciar sesión con rol de administrador Dell

1 Cierre la sesión de la consola de administración.

2 Inicie sesión en la consola de administración con las credenciales de usuario de dominio.

Haga clic en "?" en la esquina superior derecha de la consola de administración para iniciar *AdminHelp*. Aparecerá la página *Introducción*. Haga clic en **Agregar dominios**.

Se establecieron las políticas de base de su organización, pero se deben modificar de acuerdo con sus necesidades específicas, como se indica a continuación (las licencias y los derechos rigen todas las activaciones):

- El cifrado basado en políticas se habilitará con el cifrado de clave común
- Se cifran los equipos que tienen unidades de cifrado automático
- No se habilita la administración de BitLocker
- No se habilita Advanced Threat Prevention
- La protección contra amenazas está deshabilitada
- No se cifran los soportes externos
- El control de puerto no administrará los puertos

- Los dispositivos con cifrado completo de disco instalado no se cifrarán
- Data Guardian está deshabilitado

Consulte el tema de AdminHelp *Administrar políticas* para ver las descripciones de políticas.

Confirmar políticas

Confirmar políticas cuando haya finalizado la instalación.

Para confirmar políticas tras la instalación o, más tarde, una vez que se hayan guardado las modificaciones de políticas, siga estos pasos:

1 En el panel izquierdo, haga clic en **Administración** > **Confirmar**.
2 En *Comentarios*, ingrese una descripción del cambio.
3 Haga clic en **Confirmar políticas**.

7

Puertos

La siguiente tabla describe cada componente y su función.

Nombre	Puerto predeterminado	Descripción
Servicio ACL	TCP/ 8006	Administra diversos permisos y accesos a grupos de varios productos de seguridad de Dell.
Compliance Reporter	HTTP(S)/ 8084	Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías.
Consola de administración	HTTPS/ 8443	Consola de administración y centro de control para implementación en toda la empresa.
Core Server	HTTPS/ 8887 (cerrado)	Administra el flujo de políticas, las licencias y el registro para Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat Prevention. Procesa los datos de inventario para que los utilice Compliance Reporter y la consola de administración. Recopila y almacena datos de autenticación. Controla el acceso basado en roles.
Core Server HA (Alta disponibilidad)	HTTPS/ 8888	Un servicio de alta disponibilidad que permite seguridad y rendimiento aumentados para las conexiones HTTPS con la consola de administración, la autenticación previa al arranque, SED Management, FDE, BitLocker Manager, Threat Protection y Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, los productos de Data Guardian y la comunicación de SED-PBA.
Compatibility Server	TCP/ 1099 (cerrado)	Un servicio para administrar la arquitectura empresarial. Recopila y almacena los datos de inventario iniciales durante la activación y los datos de políticas durante las migraciones. Procesa datos según los grupos de usuario.
Message Broker Service	TCP/ 61616 (cerrado) y STOMP/ 61613 (cerrado, o si está configurado para DMZ, 61613 está abierto)	Maneja la comunicación entre los servicios de Dell Server. Organiza la información de políticas que se crea con el Compatibility Server para poner en cola el Policy Proxy.
Identity Server	8445 (cerrado)	Maneja las solicitudes de autenticación de dominio, incluida la autenticación de SED Management.

Nombre	Puerto predeterminado	Descripción
Forensic Server	HTTPS/ 8448	Permite a los administradores que tienen los privilegios adecuados obtener las claves de cifrado de la consola de administración para utilizarlas en los desbloqueos de datos o las tareas de descifrado. Se necesita para la API de Forensic.
Inventory Server	8887	Procesa la cola de inventario.
Policy Proxy	TCP/ 8000	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario. Se necesita para Encryption Enterprise (Windows y Mac)
PostGres	TCP/ 5432	Base de datos local utilizada para los datos de eventos.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Puerto 389: este puerto se utiliza para solicitar información desde la controladora de dominio local. Las solicitudes LDAP enviadas al puerto 389 se pueden utilizar para buscar objetos solo en el dominio de inicio del catálogo general. Sin embargo, la aplicación solicitante puede obtener todos los atributos para dichos objetos. Por ejemplo, se puede utilizar una solicitud al puerto 389 para obtener un departamento de usuario. Puerto 3268: este puerto se utiliza para solicitudes destinadas específicamente para el catálogo general. Las solicitudes LDAP enviadas al puerto 3268 se pueden utilizar para buscar objetos en todo el bosque. Sin embargo, solo se pueden devolver los atributos marcados para la replicación en el catálogo general. Por ejemplo, el departamento de un usuario no se puede devolver si utiliza el puerto 3268 ya que este atributo no se replica en el catálogo general.
Autenticación del cliente	HTTPS/ 8449	Permite la autenticación de los servidores cliente en Dell Server. Se necesita para Server Encryption
Aviso de devolución de llamada	HTTP/TCP 8446	En un servidor front-end, permite insertar un aviso de devolución de llamada en cada archivo de Office protegido, al ejecutar Data Guardian en el modo de Office protegido.