Dell Security Management Server

Guía de instalación y migración 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

Introducción

Acerca de Servidor de administración de seguridad

Servidor de administración de seguridad tiene las siguientes funciones:

- Administración centralizada de dispositivos, usuarios y políticas de seguridad
- Auditoría y elaboración de informes de cumplimiento centralizados
- Separación de tareas administrativas
- Creación y administración de políticas de seguridad basadas en roles
- Distribuye las políticas de seguridad cuando los clientes se conectan
- Recuperación de dispositivos asistida por el administrador
- Rutas de confianza para comunicación entre los componentes
- Generación de claves únicas de cifrado y depósito automático de claves seguras

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 y arquitectura

En esta sección se indican los requisitos de hardware y software, y las recomendaciones de diseño de arquitectura para la implementación de Dell Security Management Server.

Diseño de arquitectura de Security Management Server

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 muestran configuraciones de hardware sugeridas que son adecuadas para la mayoría de los ambientes.

Servidor de administración de seguridad

- Sistema operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Equipo virtual/físico
- CPU: 4 núcleos
- RAM de 16 GB:
- Unidad C: 30 GB de espacio disponible en el disco para los registros y las bases de datos de aplicaciones

NOTA: Se puede consumir hasta 10 GB para bases de datos de un evento local almacenadas en PostgreSQL.

Proxy Server

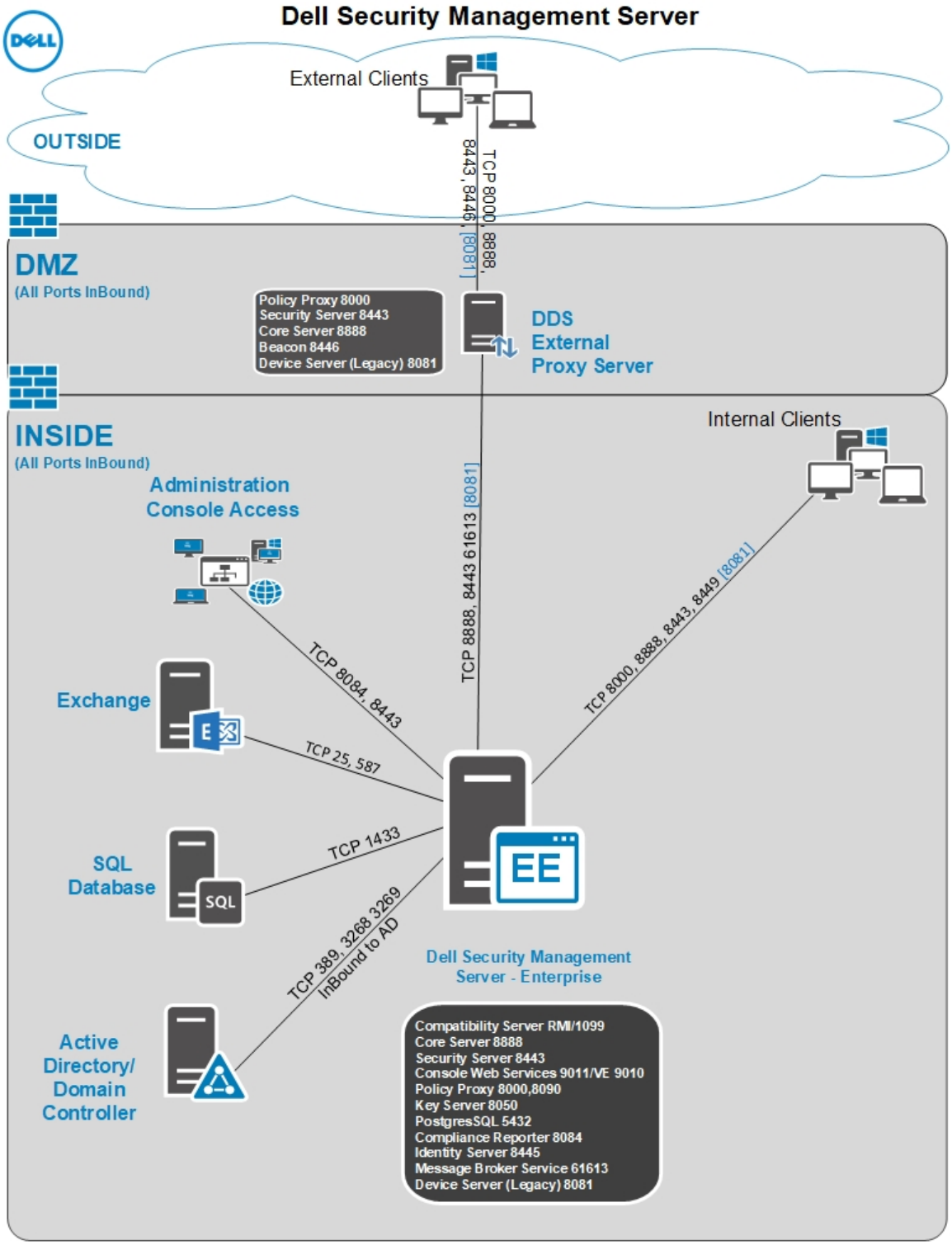
- Sistema operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Equipo virtual/físico
- CPU: 2 núcleos
- RAM: 8 GB
- Unidad C: 20 GB de espacio disponible en el disco para los registros

Especificaciones de hardware de SQL Server

- CPU: 4 núcleos
- RAM: 24 GB
- Unidad de datos: de 100 a 150 GB de espacio disponible en el disco (puede variar de acuerdo con el entorno)
- Unidad de registro: 50 GB de espacio disponible en el disco (puede variar de acuerdo con el entorno)

NOTA: Dell recomienda seguir las prácticas recomendadas para SQL Server, aunque la información mencionada anteriormente debe cubrir la mayoría de entornos.

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



NOTA: Si la organización tiene más de 20.000 extremos, póngase en contacto con Dell ProSupport para recibir ayuda.

Requisitos

Los requisitos de hardware y software para la instalación del software de Servidor de administración de seguridad se indican a continuación.

Antes de comenzar la instalación, asegúrese de que se hayan aplicado todas las revisiones y actualizaciones a los servidores utilizados para la instalación.

Hardware

En la siguiente tabla se indican los requisitos *mínimos* de hardware de Servidor de administración de seguridad. Consulte Diseño de arquitectura de Security Management Server para obtener información adicional con respecto al ajuste según el tamaño de la implementación.

Requisitos de Hardware
Procesador
CPU moderna de cuatro núcleos (1,5 GHz+)
RAM
16 GB
Espacio libre en disco
20 GB de espacio libre en el disco
NOTA: Se puede consumir hasta 10 GB para bases de datos de un evento local almacenadas en PostgreSQL
Tarjeta de red
10/100/1000 o superior
Varios
Requiere un ambiente IPv4 o IPv6 o IPv4/IPv6 híbridos

En la siguiente tabla se indican los requisitos *mínimos* de hardware para un servidor proxy front-end y back-end de Servidor de administración de seguridad.

Requisitos de Hardware
Procesador
CPU de doble núcleo moderna
RAM
8 GB
Espacio libre en disco
20 GB de espacio disponible en el disco para archivos de registro
Tarjeta de red
10/100/1000 o superior
Varios
Requiere un ambiente IPv4 o IPv6 o IPv4/IPv6 híbridos

Virtualización

Servidor de administración de seguridad se puede instalar en un entorno virtual. Solo se recomiendan los siguientes entornos.

Servidor de administración de seguridad v10.2.5 se validó para las siguientes plataformas.

Hyper-V Server está instalado como una instalación completa o básica, o como una función en Windows Server 2012, Windows Server 2016 o Windows Server 2019.

- Hyper-V Server
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - Hardware que cumpla con los requisitos mínimos de Hyper-V
  - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
  - Debe ejecutarse como una máquina virtual de generación 1
  - Visite https://technet.microsoft.com/en-us/library/hh923062.aspx para obtener más información

Servidor de administración de seguridad v10.2.5 se validó con VMware ESXi 5.5, VMware ESXi 6.0 y VMware ESXi 6.5.

NOTA: Cuando se ejecutan VMware ESXi y Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019, se recomiendan adaptadores Ethernet VMXNET3.

- 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
  - 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
- 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
  - 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 6.5
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - 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-65/index.jsp para obtener más información

NOTA: La base de datos de SQL Server que aloje Servidor de administración de seguridad debe ejecutarse en una computadora independiente por motivos de rendimiento.

SQL Server

En entornos más grandes, se recomienda encarecidamente que el servidor de la base de datos SQL se ejecute en un sistema redundante, como el clúster SQL, para asegurar la continuidad de los datos y disponibilidad. También se recomienda realizar copias de seguridad completas diariamente con inicios de sesión transaccionales habilitados para asegurar que cualquier clave generada recientemente mediante la activación del dispositivo/usuario se puede recuperar.

En las tareas de mantenimiento de la base de datos se deben incluir la reconstrucción de los índices de la base de datos y la recopilación de estadísticas.

Software

En la siguiente tabla se indican los requisitos de software de Servidor de administración de seguridad y el servidor proxy.

NOTA: Debido a la naturaleza confidencial de los datos que contiene el Security Management Server y a fin de ajustarse a la regla de privilegio mínimo, Dell recomienda la instalación del Security Management Server en su propio sistema operativo dedicado o para ser parte de un servidor de aplicaciones que tenga funciones y derechos limitados y activados que ayude a garantizar que el ambiente sea seguro. Esto incluye la no instalación de Security Management Server en servidores con infraestructuras privilegiadas. Consulte https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models para obtener más información sobre la implementación de la regla de privilegio mínimo.

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.

NOTA: Ubicaciones de registro de Policy Proxy (si está instalado): HKLM\SOFTWARE\Wow6432Node\Dell

NOTA: Ubicación de registro de los servidores Windows: HKLM\SOFTWARE\Dell

Requisitos previos

- **Paquete redistribuible de Visual C++ 2010**

  Si falta este componente, el instalador lo agregará a la instalación en el sistema.
- **Paquete redistribuible de Visual C++ 2013**

  Si falta este componente, el instalador lo agregará a la instalación en el sistema.
- **Paquete redistribuible de Visual C++ 2015**

  Si falta este componente, el instalador lo agregará a la instalación en el sistema.
- **.NET Framework versión 3.5 SP1**
- **.NET Framework versión 4.5**

  Microsoft ha publicado actualizaciones de seguridad para .NET Framework versión 4,5.
- **SQL Native Client 2012**

  Si utiliza SQL Server 2012 o SQL Server 2016.

  Si falta este componente, el instalador lo agregará a la instalación en el sistema.

Servidor de administración de seguridad: servidor back-end y servidor front-end de Dell

- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2019**
  - Standard Edition
  - Datacenter Edition

Repositorio LDAP

- Active Directory 2008 R2
- Active Directory 2012 R2
- Active Directory 2016

Consola de administración y Compliance Reporter

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

NOTA: Su explorador debe aceptar cookies.

Entornos virtuales recomendados para los componentes Servidor de administración de seguridad

Servidor de administración de seguridad se puede instalar en un entorno virtual.

Actualmente, Dell es compatible con el alojamiento de Dell Security Management Server o Dell Security Management Server Virtual dentro de un entorno de infraestructura como servicio (IaaS) alojado en la nube, como Amazon Web Services, Azure y varios otros proveedores. La compatibilidad con estos entornos es limitada debido a la funcionalidad de Security Management Server. El administrador de la solución IaaS se encargará de la administración y seguridad de estas máquinas virtuales.

Requisitos adicionales de infraestructura. Los requisitos adicionales de infraestructura, como Active Directory y SQL Server, se siguen solicitando para que el funcionamiento sea correcto.

NOTA: La base de datos de SQL Server que aloje Servidor de administración de seguridad debe estar ejecutándose en una computadora independiente.

Base de datos

- **SQL Server 2008 R2:** Standard Edition/Enterprise Edition
- **SQL Server 2012** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2014** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2016** Standard Edition / Enterprise Edition
- **SQL Server 2017** Standard Edition / Enterprise Edition

NOTA: No son compatibles las versiones Express Edition en entornos de producción. El uso de las versiones Express Edition se debe limitar a pruebas de concepto (POC) y a efectos de evaluación.

NOTA: A continuación, se muestran los requisitos para los permisos SQL. El usuario que esté ejecutando la instalación y los servicios debe tener derechos de administrador local. Además, se requieren derechos de administrador local para la cuenta de servicio que administra los servicios de Dell Security Management Server.

Tipo	Acción	Caso	Se necesita el privilegio SQL
Back-end	Actualización	Por definición, las actualizaciones ya tienen establecidos los DB e inicio de sesión/usuario	db_owner
Back-end	Restaurar instalación	La restauración implica un DB e inicio de sesión existentes	db_owner
Back-end	Nueva instalación	Usar una DB existente	db_owner
Back-end	Nueva instalación	Crear una DB nueva	dbcreator, db_owner
Back-end	Nueva instalación	Utilizar un inicio de sesión existente	db_owner
Back-end	Nueva instalación	Crear nuevo inicio de sesión	securityadmin
Back-end	Desinstalar	NA	NA
Proxy de front end	Cualquiera	NA	NA

NOTA: Si el control de cuentas de usuario (UAC) está habilitado, debe deshabilitarlo antes de la instalación en Windows Server 2012 R2 cuando lo instale en C:\Program Files. El servidor debe reiniciarse para que el cambio tenga efecto.

Durante la instalación, se requieren las credenciales de autenticación de Windows o SQL para configurar la base de datos Independientemente del tipo de credenciales que se utilizan, la cuenta debe tener los privilegios adecuados para la acción que se realiza. En la tabla anterior se indican los privilegios obligatorios para cada tipo de instalación. Además, la cuenta que se utiliza para crear y configurar la base de datos debe tener el esquema predeterminado establecido en dbo.

Estos privilegios solo se solicitan durante la instalación a fin de configurar la base de datos. Una vez que Security Management Server se instala, la cuenta que se utiliza para administrar el acceso a SQL se puede restringir a db_owner y las funciones públicas.

Si no está seguro sobre los privilegios de acceso o la conectividad a la base de datos, pídale al administrador de la base datos que los confirme antes de iniciar la instalación.

Compatibilidad de idiomas de la consola de administración

La consola de administración es compatible con la interfaz de usuario multilingüe (MUI) y con los siguientes idiomas:

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

3

Configuración previa a la instalación

Antes de empezar, lea las *consultas técnicas de Servidor de administración de seguridad* para ver las soluciones alternativas actuales o los problemas conocidos relacionados con Servidor de administración de seguridad.

La configuración previa a la instalación del servidor o los servidores en los que tiene pensado instalar Servidor de administración de seguridad es muy importante. Preste especial atención a esta sección para garantizar una instalación fluida de Servidor de administración de seguridad.

Configuración

1 Si está habilitado, desactive Configuración de seguridad mejorada (ESC) de Internet Explorer. En las opciones de seguridad del navegador, incorpore la URL de Dell Server a los sitios de confianza. Reinicie el servidor.

2 Abra los siguientes puertos para cada componente:

Interno:

Comunicación de Active Directory: TCP/389

Comunicación por correo electrónico (opcional): 25

A front-end (si fuera necesario):

Comunicación de Policy Proxy externo con Message Broker: STOMP/61613

Comunicación con el servidor de seguridad de back-end: HTTPS/8443

Comunicación con el Core Server de back-end: HTTPS/8888

Comunicación con los puertos RMI - 1099

Comunicación con el servidor de dispositivos de back-end: HTTP(S)/8443; si Servidor de administración de seguridad es v7.7 o posterior. Si su Dell Server es anterior a v7.7, HTTP(S)/8081.

Servidor de punto de referencia: HTTP/8446 (si se utiliza Data Guardian)

Externo (si fuera necesario):

Base de datos de SQL: TCP/1433

Consola de administración: HTTPS/8443

LDAP: TCP/389/636 (controladora de dominio local), TCP/3268/3269 (catálogo general), TCP/135/49125+ (RPC)

Compatibility Server: TCP/1099

Compliance Reporter: HTTP(S)/8084 (se configura automáticamente en la instalación)

Identity Server: HTTPS/8445

Core Server: HTTPS/8888 (8888 se configura automáticamente en la instalación)

Device Server: HTTP(S)/8443 (Servidor de administración de seguridad v7.7 o posterior) o HTTP(S)/8081 (anterior a Dell Server v7.7)

Key Server: TCP/8050

Policy Proxy: TCP/8000

Security Server: HTTPS/8443

Autenticación de cliente: HTTPS/8449 (si se utiliza Server Encryption)

Comunicación de cliente, si se utiliza Advanced Threat Prevention: HTTPS/TCP/443

Creación de una base de datos de Dell Server

3 Estas instrucciones son opcionales. El instalador crea una base de datos si todavía no existe una. Si prefiere configurar una base de datos antes de instalar Servidor de administración de seguridad, siga las instrucciones que se indican a continuación para crear la base de datos SQL y el usuario SQL en SQL Management Studio.

Cuando instale Servidor de administración de seguridad, siga las instrucciones de Instalación del servidor back-end con base de datos existente.

Servidor de administración de seguridad está preparado para la autenticación de SQL y Windows. El método de autenticación predeterminado corresponde a la autenticación de SQL.

Tras crear la base de datos, cree un usuario de base de datos Dell con derechos db_owner. La función db_owner puede asignar permisos, hacer copias de seguridad y restaurar la base de datos, crear y eliminar objetos y administrar cuentas de usuario y roles sin restricciones. Además, asegúrese de que este usuario tiene permisos/privilegios para ejecutar procedimientos almacenados.

Al utilizar una instancia de SQL Server no predeterminada, tras la instalación de Servidor de administración de seguridad, debe especificar cuál es el puerto dinámico de la instancia en la pestaña Base de datos de la Herramienta de configuración del servidor. Para obtener más información, consulte Herramienta de configuración del servidor. Como alternativa, habilite el servicio SQL Server Browser y asegúrese de que el puerto UDP 1434 esté abierto. Para obtener más información, consulte https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

La intercalación "SQL_Latin1_General_CP1_CI_AS" corresponde a la intercalación esperada, no predeterminada, compatible con la base de datos o la instancia de SQL.

Para crear la base de datos de SQL y el usuario de SQL en SQL Management Studio, elija entre:

Instalación de los paquetes redistribuibles de Visual C++ 2010/2013/2015

4 *Si todavía no lo ha hecho*, instale los paquetes redistribuibles de Visual C++ 2010, 2013 y 2015. Si lo desea, puede permitir que el instalador de Servidor de administración de seguridad instale estos componentes.

Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019: https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads

Instalar .NET Framework 4.5

5 *Si aún no estuviera instalado*, instale .NET Framework 4.5.

Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019: https://www.microsoft.com/en-us/download/details.aspx?id=30653

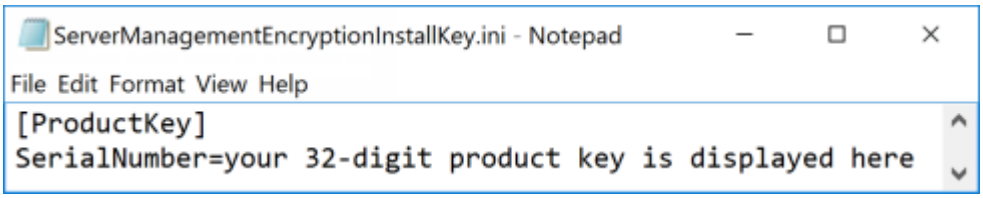
Instalación de SQL Native Client 2012

6 *Si utiliza SQL Server 2012 o SQL Server 2016*, instale SQL Native Client 2012. Si lo desea, puede permitir que el instalador de Servidor de administración de seguridad instale este componente.

http://www.microsoft.com/en-us/download/details.aspx?id=35580

Opcional

7 **Para una instalación nueva**: copie su clave de producto (el nombre del archivo es *EnterpriseServerInstallKey.ini*) en **C:\Windows** para rellenar automáticamente la clave de producto de 32 caracteres en el instalador de Servidor de administración de seguridad.



La configuración previa a la instalación del servidor ha finalizado. Continúe en Instalar o actualizar/migrar.

4

Instalación o actualización/migración

Este capítulo proporciona instrucciones para realizar lo siguiente:

- Nueva instalación: para instalar un nuevo Servidor de administración de seguridad.
- Actualización/migración: para actualizar desde un Enterprise Server v9.2 o posterior existente y funcional.
- Desinstalación de Security Management Server: para eliminar la instalación actual, si es necesario.

Si en la instalación se debe incluir más de un servidor principal (back-end), comuníquese con su representante de Dell ProSupport.

Antes de comenzar la instalación o la actualización/migración

Antes de empezar, asegúrese de que se completen los pasos de Configuración previa a la instalación aplicables.

Lea las consultas técnicas de *Servidor de administración de seguridad* para ver las soluciones alternativas actuales o los problemas conocidos relacionados con la instalación de Servidor de administración de seguridad.

Para disminuir el tiempo de instalación en Server 2016, agregue las siguientes exclusiones a Windows Defender:

- C:\Program Files\Dell\Enterprise Edition
- C:\Windows\Installer
- La ruta de acceso de archivo desde la que se ejecuta el instalador

Dell recomienda que se utilicen las prácticas recomendadas de la base de datos para la base de datos de Dell Server y que se incluya el software de Dell en el plan de recuperación ante desastres de su organización.

Si desea implementar componentes Dell en la DMZ, asegúrese de que estén protegidos apropiadamente frente a ataques.

Para producción, Dell recomienda encarecidamente la instalación de SQL Server en un servidor dedicado.

Una práctica recomendada corresponde a la instalación del servidor de back-end antes de instalar y configurar un servidor de front-end.

Los archivos de registro de instalación se encuentran en este directorio: **C:\Users\<LoggedOnUser>\AppData\Local\Temp**

Nueva instalación

Seleccione una de estas dos opciones para la instalación del servidor de back-end:

- Instalación del servidor back-end y una base de datos nueva: para instalar un nuevo Servidor de administración de seguridad y una nueva base de datos.
- Instalación del servidor back-end con base de datos existente: para instalar un nuevo Servidor de administración de seguridad y conectarse a una base de datos SQL creada durante Configuración previa a la instalación o una base de datos SQL existente que sea v9.x o una versión posterior, cuando la versión del esquema coincida con la versión de Servidor de administración de seguridad que se va a instalar. Se debe migrar una base de datos 9.2 o una versión posterior al esquema más reciente con la versión más reciente de la Herramienta de configuración del servidor. Para obtener instrucciones sobre la migración de bases de datos con la Herramienta de configuración del servidor, consulte Migración de la base de datos. Para obtener la Herramienta de configuración del servidor más reciente, o para migrar una base de datos pre-v9.2, póngase en contacto con Dell ProSupport para obtener asistencia.

NOTA:

Si tiene un Enterprise Server v9.2 o una versión posterior que funcione, consulte las instrucciones en **Actualización/migración de servidores back-end**.

Si instala un servidor de front-end, realice esta instalación después de la instalación del servidor de back-end:

- Instalación del servidor de front-end: para instalar un servidor de front-end para que se comunique con un servidor de back-end.

Instalación del servidor back-end y una base de datos nueva

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 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 En el cuadro de diálogo *Bienvenido*, haga clic en **Siguiente**.

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

7 Si opcionalmente copió el archivo EnterpriseServerInstallKey.ini en C:\Windows tal como se explica en Configuración previa a la instalación, haga clic en **Siguiente**. En caso contrario, 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 back-end** y haga clic en **Siguiente**.

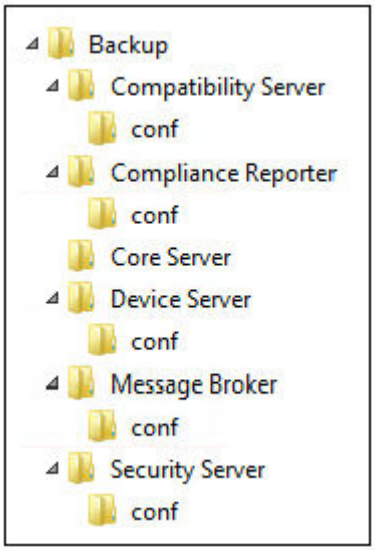
9 Para instalar Servidor de administración de seguridad en la ubicación predeterminada de C:\Program Files\Dell, haga clic en **Siguiente**. De lo contrario, haga clic en **Cambiar** para seleccionar otra ubicación y, a continuación, haga clic en **Siguiente**.

10 Para seleccionar una ubicación en la que guardar los archivos de configuración de copia de seguridad, haga clic en **Cambiar**, navegue hasta la carpeta deseada y, a continuación, haga clic en **Siguiente**.

Dell recomienda seleccionar una ubicación de red remota o unidad externa para la copia de seguridad.

Tras la instalación, cualquier cambio realizado a los archivos de configuración, incluidos los cambios realizados con la Herramienta de configuración del servidor, deberán ser guardados mediante una copia de seguridad manual en estas carpetas. Los archivos de configuración son una parte importante de toda la información que se utiliza para restaurar manualmente Dell Server, si es necesario.

NOTA: La estructura de carpetas creada por el instalador durante este paso de la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable.



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

Haga clic en **Examinar** para ingresar la ruta al certificado.

Ingrese la contraseña asociada con este certificado. El archivo de almacenamiento de claves debe ser .p12 o pfx. Para obtener instrucciones, consulte la sección Exportación de un certificado a .PFX mediante la consola de administración de certificados.

Haga clic en **Siguiente**.

> **NOTA:**
>
> Para utilizar este valor, el certificado CA exportado que se importe debe tener la cadena de confianza completa. Si no está seguro, vuelva a exportar el certificado CA y asegúrese de que estén seleccionadas las siguientes opciones en el "Asistente para exportar certificados":
>
> - Personal Information Exchange: PKCS#12 (.PFX)
> - Si es posible, incluir todos los certificados en la ruta de acceso de certificación
> - Exportar todas las propiedades extendidas

O bien

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.

12 Para Server Encryption, tiene una opción de escoger los tipos de certificados digitales que se utilizarán. 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**.

Haga clic en **Examinar** para ingresar la ruta al certificado.

Ingrese la contraseña asociada con este certificado. El archivo de almacenamiento de claves debe ser .p12 o pfx. Para obtener instrucciones, consulte la sección Exportación de un certificado a .PFX mediante la consola de administración de certificados.

Haga clic en **Siguiente**.

NOTA:

Para utilizar este valor, el certificado CA exportado que se importe debe tener la cadena de confianza completa. Si no está seguro, vuelva a exportar el certificado CA y asegúrese de que estén seleccionadas las siguientes opciones en el "Asistente para exportar certificados":

- Personal Information Exchange: PKCS#12 (.PFX)
- Si es posible, incluir todos los certificados en la ruta de acceso de certificación
- Exportar todas las propiedades extendidas

O bien

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.

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

- Para aceptar los nombres de host y los puertos predeterminados, en el cuadro de diálogo *Configuración de la instalación del servidor back-end*, haga clic en **Siguiente**.
- Si está utilizando un servidor de front-end, seleccione **Funciona con front-end para comunicarse con clientes internos de la red o externos de DMZ** e ingrese el nombre de host de Security Server de front-end (por ejemplo, server.domain.com).
- Para ver o editar nombres de host, 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 guión bajo ("_").

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

- Para ver o editar puertos, haga clic en **Editar puertos**. Edite puertos solo si fuera necesario. Dell recomienda utilizar los valores predeterminados. Cuando termine, haga clic en **Aceptar**.

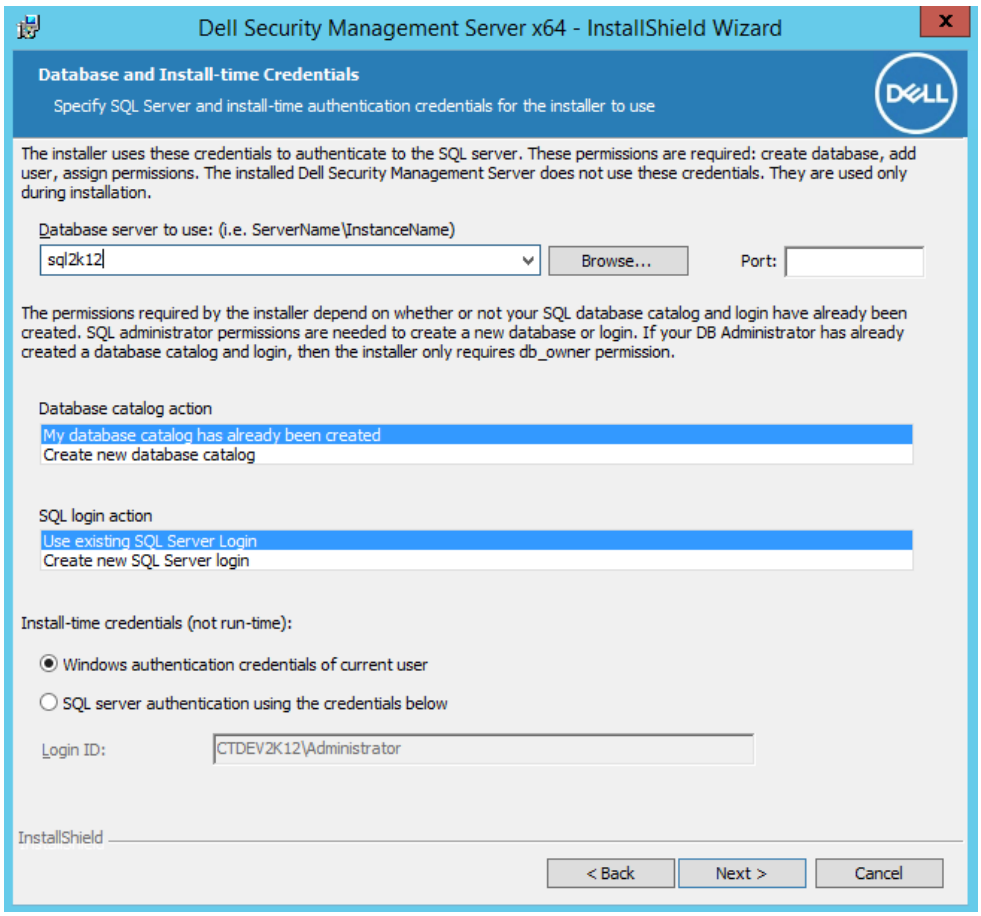
14 Para crear una nueva base de datos, siga estos pasos:

a Haga clic en **Examinar** para seleccionar el servidor en el que se instalará la base de datos.

b Seleccione el método de autenticación que el instalador debe utilizar para configurar la base de datos de Dell Server. Tras la instalación, el producto instalado no utiliza las credenciales que se especifican aquí.

- **Credenciales de autenticación de Windows del usuario actual**

  Si selecciona la autenticación de Windows, se deben utilizar las mismas credenciales que se utilizaron para iniciar sesión en Windows (*Nombre de usuario* y *Contraseña* no se pueden editar). Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server.



O bien

- **Autenticación del SQL Server mediante las siguientes credenciales**

  Si utilizara la autenticación SQL, la cuenta SQL utilizada debe tener derechos de administrador del sistema en el SQL Server.

  El instalador debe autenticar el SQL Server con los siguientes permisos: crear base de datos, agregar usuario y asignar permisos.

c Identifique el catálogo de base de datos:

Ingrese el nombre de un nuevo catálogo de base de datos. En el siguiente cuadro de diálogo se le pide crear el nuevo catálogo.

d Haga clic en **Siguiente**.

e Para confirmar que desea que el instalador cree una base de datos, haga clic en **Sí**. Para volver a la pantalla anterior para realizar cambios, haga clic en **No**.

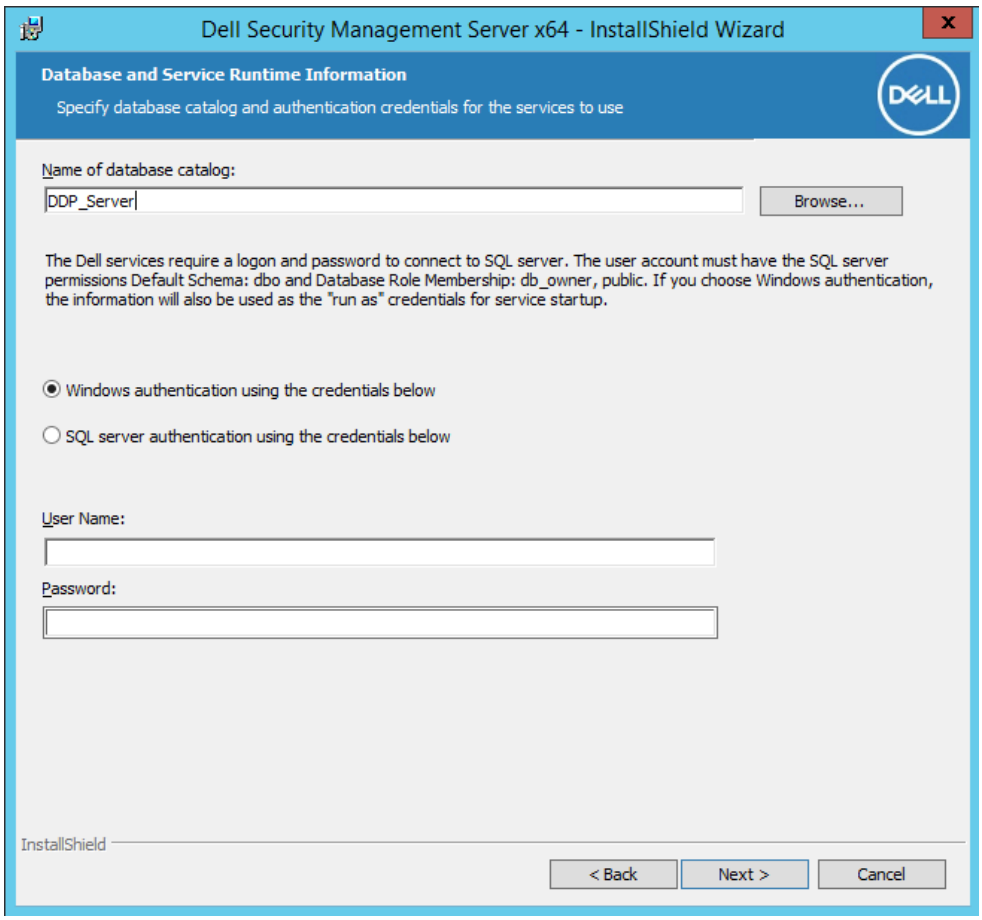
15 Seleccione el método de autenticación que utilizará el producto. Este paso conecta una cuenta al producto.

- **Autenticación de Windows**

Seleccione **Autenticación Windows mediante las credenciales siguientes,** ingrese las credenciales del producto que desea utilizar y haga clic en **Siguiente**.

Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server. La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

Estas credenciales también las utilizan los servicios de Dell a medida que trabajen con Servidor de administración de seguridad.



O bien

- **Autenticación SQL Server**

  Seleccione **Autenticación SQL Server con las siguientes credenciales**, ingrese las credenciales de SQL Server para que los servicios de Dell las utilicen a medida que funcionan con Servidor de administración de seguridad y haga clic en **Siguiente**.

  La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

16 En el cuadro de diálogo *Preparado para instalar el programa*, haga clic en **Instalar**.
El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de instalación.

17 Cuando se complete la instalación, haga clic en **Finalizar**.
Las tareas de instalación del servidor back-end se han completado.

Dell Services se reinicia al final de la instalación. No es necesario reiniciar Dell Server.

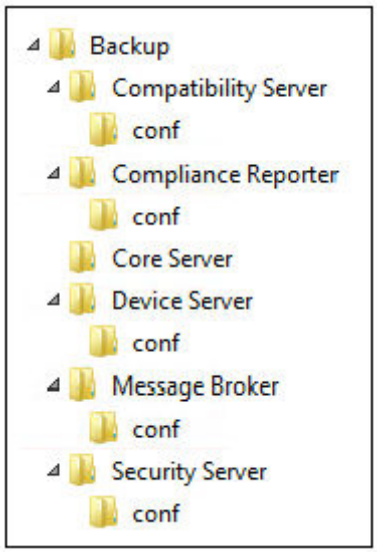
Instalación del servidor back-end con base de datos existente

NOTA:
Si tiene un Dell Server v9.2 o una versión posterior que funcione, consulte las instrucciones en Actualización/migración de servidores back-end.

Puede instalar un nuevo Servidor de administración de seguridad y conectarse a una base de datos SQL creada durante Configuración previa a la instalación o una base de datos SQL existente que sea v9.x o una versión posterior, cuando la versión del esquema coincida con la versión de Servidor de administración de seguridad que se va a instalar.

La cuenta de usuario desde la que se está realizando la instalación debe tener privilegios de propietario de la base de datos para la base de datos SQL. Si no está seguro sobre los privilegios de acceso o la conectividad a la base de datos, pídale al administrador de la base datos que los confirme antes de iniciar la instalación.

Si la base de datos existente se ha instalado previamente con Servidor de administración de seguridad, antes de empezar la instalación, asegúrese de realizar una copia de seguridad de la base de datos, archivos de configuración y secretKeyStore y que se pueda acceder a ellos desde el servidor en el que esté instalando Servidor de administración de seguridad. Acceda a estos archivos en caso necesario para configurar Servidor de administración de seguridad y la base de datos existente. La estructura de carpetas creada por el instalador durante la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable.



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 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. En el cuadro de diálogo *Bienvenido*, haga clic en **Siguiente**.
6. Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
7. Si opcionalmente copió el archivo **EnterpriseServerInstallKey.ini** en **C:\Windows** tal como se explica en Configuración previa a la instalación, haga clic en **Siguiente**. En caso contrario, 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 back-end** e **Instalación de recuperación** y haga clic en **Siguiente**.

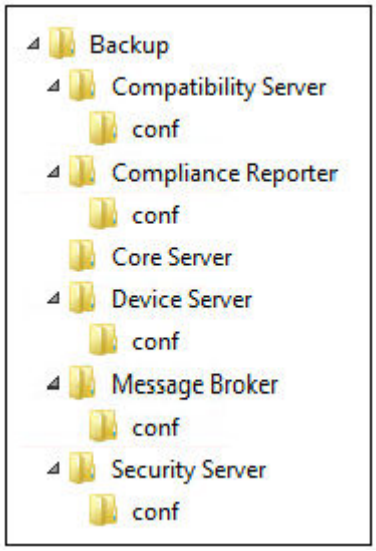
9 Para instalar Servidor de administración de seguridad en la ubicación predeterminada de C:\Program Files\Dell, haga clic en **Siguiente**. En caso contrario, haga clic en **Cambiar** para seleccionar una ubicación diferente y, a continuación, haga clic en **Siguiente**.

10 Para seleccionar una ubicación en la que guardar los archivos de configuración de copia de seguridad, haga clic en **Cambiar**, navegue hasta la carpeta deseada y, a continuación, haga clic en **Siguiente**.

Dell recomienda seleccionar una ubicación de red remota o unidad externa para la copia de seguridad.

Tras la instalación, cualquier cambio realizado a los archivos de configuración, incluidos los cambios realizados con la Herramienta de configuración del servidor, deberán ser guardados mediante una copia de seguridad manual en estas carpetas. Los archivos de configuración son una parte importante de la información total utilizada para restaurar de forma manual el Dell Server.

NOTA: La estructura de carpetas creada por el instalador durante la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable.



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

Haga clic en **Examinar** para ingresar la ruta al certificado.

Ingrese la contraseña asociada con este certificado. El archivo de almacenamiento de claves debe ser .p12 o pfx. Para obtener instrucciones, consulte la sección Exportación de un certificado a .PFX mediante la consola de administración de certificados.

Haga clic en **Siguiente**.

NOTA:

Para utilizar este valor, el certificado CA exportado que se importe debe tener la cadena de confianza completa. Si no está seguro, vuelva a exportar el certificado CA y asegúrese de que estén seleccionadas las siguientes opciones en el "Asistente para exportar certificados":

- Personal Information Exchange: PKCS#12 (.PFX)
- Si es posible, incluir todos los certificados en la ruta de acceso de certificación
- Exportar todas las propiedades extendidas

O bien

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.

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

- Para aceptar los nombres de host y los puertos predeterminados, en el cuadro de diálogo *Configuración de la instalación del servidor back-end*, haga clic en **Siguiente**.
- Si está utilizando un servidor de front-end, seleccione **Funciona con front-end para comunicarse con clientes internos de la red o externos de DMZ** e ingrese el nombre de host de Security Server de front-end (por ejemplo, server.domain.com).
- Para ver o editar nombres de host, 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 ("_").

  Cuando termine, haga clic en **Aceptar**.
- Para ver o editar puertos, haga clic en **Editar puertos**. Edite puertos solo si fuera necesario. Dell recomienda utilizar los valores predeterminados. Cuando termine, haga clic en **Aceptar**.

13 Especifique el método de autenticación que utilizará el instalador.

a Haga clic en **Examinar** para seleccionar el servidor donde reside la base de datos.

b Seleccione el tipo de autenticación.

- **Credenciales de autenticación de Windows del usuario actual**

  Si selecciona la autenticación de Windows, se utilizan las mismas credenciales que se utilizaron para iniciar sesión en Windows (*Nombre de usuario* y *Contraseña* no se pueden editar). Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server.

  O bien

- **Autenticación del SQL Server mediante las siguientes credenciales**

  Si utilizara la autenticación SQL, la cuenta SQL utilizada debe tener derechos de administrador del sistema en el SQL Server.

  El instalador debe autenticar el SQL Server con los siguientes permisos: crear base de datos, agregar usuario y asignar permisos.

c Haga clic en **Examinar** para seleccionar el nombre del catálogo de base de datos existente.

d Haga clic en **Siguiente**.

14 Si se muestra el cuadro de diálogo Error de base de datos existente, seleccione la opción adecuada.

Si el instalador detecta un problema con la base de datos, se mostrará el cuadro de diálogo *Error de base de datos existente*. Las opciones del cuadro de diálogo dependerán de estas circunstancias:

- El esquema de la base de datos es de una versión anterior. (Consulte el paso a).
- La base de datos ya tiene un esquema de base de datos que coincide con la versión que se está instalando. (Consulte el paso b.)

a Cuando el esquema de la base de datos es de una versión anterior, seleccione **Salir del instalador para finalizar esta instalación**. A continuación, deberá realizar una copia de seguridad de la base de datos.

Las siguientes opciones DEBEN utilizarse solo con la ayuda de Dell ProSupport:

- La opción **Migrar esta base de datos al esquema actual** se utiliza para recuperar una buena base de datos desde una implementación errónea del servidor. Esta opción utiliza los archivos de configuración en la carpeta /Copia de seguridad para reconectar a la base de datos y, a continuación, migrar la base de datos al esquema actual. Esta opción se deberá utilizar *solo* después de intentar primero la reinstalación de la versión correcta de Servidor de administración de seguridad y, a continuación, ejecutar el instalador más reciente para actualizar.
- La opción **Continuar sin migrar la base de datos** instala los archivos de Servidor de administración de seguridad sin configurar completamente la base de datos. La configuración de la base de datos se debe realizar más tarde de forma manual mediante la herramienta de configuración del servidor y requerirá más cambios manuales.

b Cuando el esquema de la base de datos ya tiene el esquema de la versión actual, pero no está conectado al back-end de Servidor de administración de seguridad, se considera una *Recuperación.* Si **Instalación de recuperación** no estaba seleccionada en este paso, aparece este cuadro de diálogo:

- Seleccione **Modo de instalación de recuperación** para continuar la instalación con la base de datos seleccionada.
- Seleccione **Seleccionar una base de datos nueva** para elegir una base de datos diferente.
- Seleccione **Salir del instalador para finalizar esta instalación**.

c Haga clic en **Siguiente**.

15 Seleccione el método de autenticación que utilizará el producto. Esta es la cuenta que utiliza el producto para funcionar con la base de datos y los servicios de Dell.

- **Para utilizar la autenticación de Windows**

  Seleccione **Autenticación Windows mediante las credenciales siguientes,** ingrese las credenciales de la cuenta que el producto pueda utilizar y haga clic en Siguiente.

  Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server. La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

  O bien

- **Para utilizar la autenticación del SQL Server**

  Seleccione **Autenticación del SQL Server mediante las siguientes credenciales**, ingrese las credenciales del SQL Server y, a continuación, haga clic en **Siguiente.**

  La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

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

El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de instalación.

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

Las tareas de instalación del servidor back-end se completaron.

Dell Services se reinicia al final de la instalación. No es necesario reiniciar el servidor.

Instalación del servidor front-end

La instalación del servidor front-end proporciona una opción de front-end (modo DMZ) para utilizarla con Servidor de administración de seguridad. 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 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 Si opcionalmente copió el archivo EnterpriseServerInstallKey.ini en C:\Windows tal como se explica en Configuración previa a la instalación, haga clic en **Siguiente**. En caso contrario, 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**.

Haga clic en **Examinar** para ingresar la ruta al certificado.

Ingrese la contraseña asociada con este certificado. El archivo de almacenamiento de claves debe ser .p12 o pfx. Para obtener instrucciones, consulte la sección Exportación de un certificado a .PFX mediante la consola de administración de certificados.

Haga clic en **Siguiente**.

> **NOTA:**
> Para utilizar este valor, el certificado CA exportado que se importe debe tener la cadena de confianza completa. Si no está seguro, vuelva a exportar el certificado CA y asegúrese de que estén seleccionadas las siguientes opciones en el "Asistente para exportar certificados":
>
> - Personal Information Exchange: PKCS#12 (.PFX)
> - Si es posible, incluir todos los certificados en la ruta de acceso de certificación
> - Exportar todas las propiedades extendidas

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**.
El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de instalación.

14 Cuando se complete la instalación, haga clic en **Finalizar**.
Las tareas de instalación del servidor front-end se han completado.

Actualización/migración

Puede actualizar Enterprise Server v9.2 y versiones posteriores a Servidor de administración de seguridad v10.x. Si su versión de Dell Server es más antigua que v9.2, primero debe actualizarla a v9.2 y luego actualizarla a versiones más recientes.

Antes de comenzar la actualización/migración

Antes de empezar, asegúrese de que se completen los pasos de Configuración previa a la instalación aplicables.

Lea las consultas técnicas de *Servidor de administración de seguridad (Servidor de administración de seguridad)* para ver las soluciones alternativas actuales o los problemas conocidos relacionados con la instalación de Servidor de administración de seguridad.

La cuenta de usuario desde la que se está realizando la instalación debe tener privilegios de propietario de la base de datos para la base de datos SQL. Si no está seguro sobre los privilegios de acceso o la conectividad a la base de datos, pídale al administrador de la base datos que los confirme antes de iniciar la instalación.

Dell recomienda que se utilicen las prácticas recomendadas de la base de datos para la base de datos de Dell Server y que se incluya el software de Dell en el plan de recuperación ante desastres de su organización.

Si desea implementar componentes Dell en la DMZ, asegúrese de que estén protegidos apropiadamente frente a ataques.

Para producción, Dell recomienda encarecidamente la instalación de SQL Server en un servidor dedicado.

A fin de aprovechar todas las funcionalidades de las políticas, Dell recomienda actualizar a las versiones más recientes tanto de Servidor de administración de seguridad como de los clientes.

Servidor de administración de seguridad v9.x admite:

- Encryption Enterprise:
  - Clientes de Windows v7.x/8.x
  - Clientes Mac v7.x/8.x
  - Clientes SED v8.x
  - Autenticación v8.x
  - BitLocker Manager v7.2x+ y v8.x
  - Data Guardian v1.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprisev1.x
- Actualización/migración desde Servidor de administración de seguridad v9.2 o posterior. (Cuando migre desde Servidor de administración de seguridad anterior a v9.2, póngase en contacto con Dell ProSupport para obtener asistencia).

Al actualizar/migrar Servidor de administración de seguridad a una nueva versión que incluya nuevas políticas ingresadas en la nueva versión, confirme las políticas actualizadas después de la migración/actualización, a fin de garantizar que su configuración preferida de políticas se implemente para las nuevas políticas, y no los valores predeterminados.

En general, nuestra ruta de actualización recomendada es actualizar/migrar Servidor de administración de seguridad y sus componentes, seguido de la instalación/actualización del cliente.

Aplicación de cambios en la política

1 Como un administrador de Dell, inicie sesión en la Management Console.

2 En el menú izquierdo, haga clic en **Administración** > **Confirmar**.

3 En *Comentarios*, ingrese una descripción del cambio.

4 Haga clic en **Confirmar políticas**.

5 Cuando haya realizado la confirmación, cierre la sesión de la consola de administración.

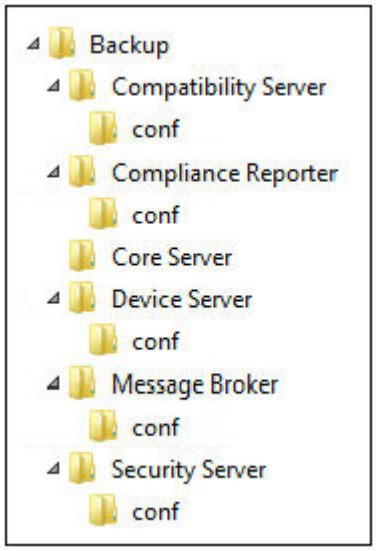
Asegurarse de que Dell Services se esté ejecutando

6 En el menú *Inicio* de Windows, haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y, si fuera necesario, haga clic en **Iniciar el servicio**.

Copia de seguridad de la instalación existente

7 Realice una copia de seguridad de toda la instalación existente en una ubicación alternativa. La copia de seguridad debe incluir la base de datos SQL, secretKeyStore y archivos de configuración. Se necesitan varios archivos de su instalación existente después de completar el proceso de actualización/migración.

> **NOTA:**
> La estructura de carpetas creada por el instalador durante la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable



Actualización/migración de servidores back-end

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 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**.

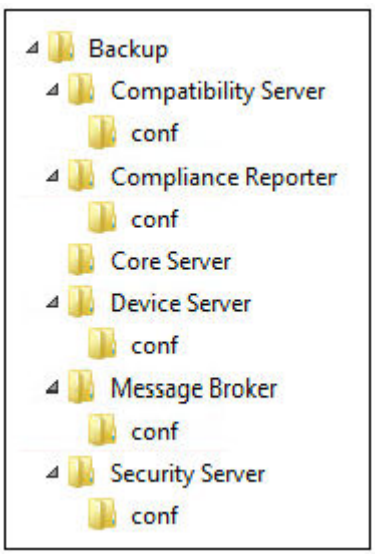
4 En el cuadro de diálogo *Bienvenido*, haga clic en **Siguiente**.

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

6 Para seleccionar una ubicación en la que guardar los archivos de configuración de copia de seguridad, haga clic en **Cambiar**, navegue hasta la carpeta deseada y haga clic en **Siguiente**.

Dell recomienda seleccionar una ubicación de red remota o unidad externa para la copia de seguridad.

La estructura de carpetas creada por el instalador durante la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable.



7 Cuando el instalador localiza correctamente la base de datos existente, el cuadro de diálogo se rellenará por usted.

Para conectarse a la base de datos existente, especifique el método de autenticación que desea utilizar. Tras la instalación, el producto instalado no utiliza las credenciales que se especifican aquí.

a Seleccione el tipo de autenticación de la base de datos:

- **Credenciales de autenticación de Windows del usuario actual**

  Si selecciona la autenticación de Windows, se deben utilizar las mismas credenciales que se utilizaron para iniciar sesión en Windows (*Nombre de usuario* y *Contraseña* no se pueden editar).

  Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server. La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

  O bien

- **Autenticación del SQL Server mediante las siguientes credenciales**

  Si utilizara la autenticación SQL, la cuenta SQL utilizada debe tener derechos de administrador del sistema en el SQL Server.

  El instalador debe autenticar el SQL Server con los siguientes permisos: crear base de datos, agregar usuario y asignar permisos.

b Haga clic en **Siguiente**.

8 Si el cuadro de diálogo Información de cuenta de tiempo de ejecución del servicio no está rellenado previamente, especifique el método de autenticación para el producto que desea utilizar después de la instalación.

a Seleccione el tipo de autenticación.

b Ingrese el nombre de usuario y la contraseña de la cuenta de servicio del dominio que los servicios de Dell utilizarán para acceder al SQL Server y haga clic en **Siguiente.**

La cuenta de usuario debe tener el formato DOMAIN\\Username y el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

9 Si no se realizara una copia de seguridad de la base de datos, ***debe*** realizarla antes de continuar con la instalación. ***La actualización de la base de datos no puede deshacerse.*** Solo después de que se haya realizado una copia de seguridad de la base de datos, seleccione **Sí, se ha realizado una copia de seguridad de la base de datos**, y haga clic en **Siguiente**.

10 Haga clic en **Instalar** para iniciar la instalación.

El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de actualización.

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

Dell Services se reinicia al final de la migración. No es necesario reiniciar Dell Server.

El instalador realizará los pasos 12-13 por usted. Es una Práctica recomendada comprobar estos valores para asegurarse de que los cambios se han realizado correctamente.

12 En la instalación a la que ha hecho copia de seguridad, copie y pegue <directorio de instalación de Compatibility Server>\conf \secretKeyStore en la nueva instalación:

<Directorio de instalación de Compatibility Server>\conf\secretKeyStore

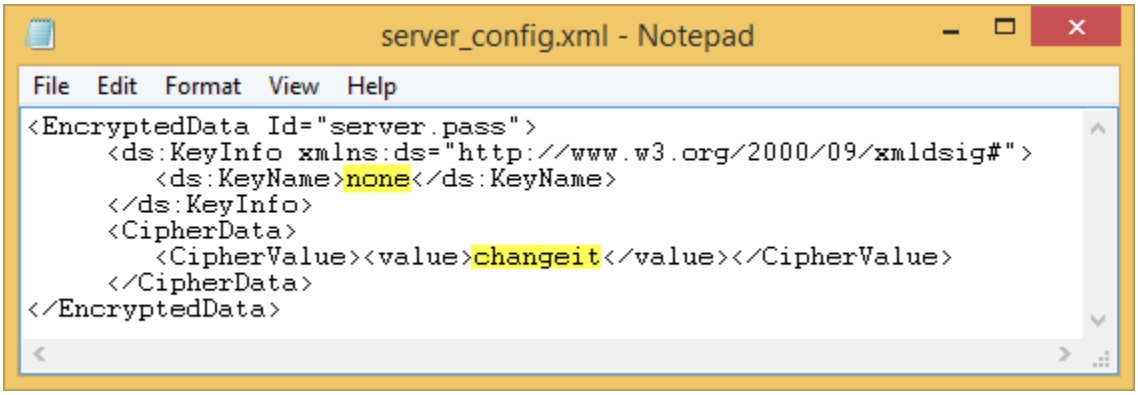
13 En la nueva instalación, abra <Directorio de instalación de Compatibility Server>\conf\server_config.xml y sustituya el valor **server.pass** por el valor del <directorio de instalación de Compatibility Server>\conf\server_config.xml del que ha hecho copia de seguridad, de la siguiente forma:

Instrucciones para server.pass:

Si conoce la contraseña, consulte el archivo server_config.xml de ejemplo y realice los siguientes cambios:

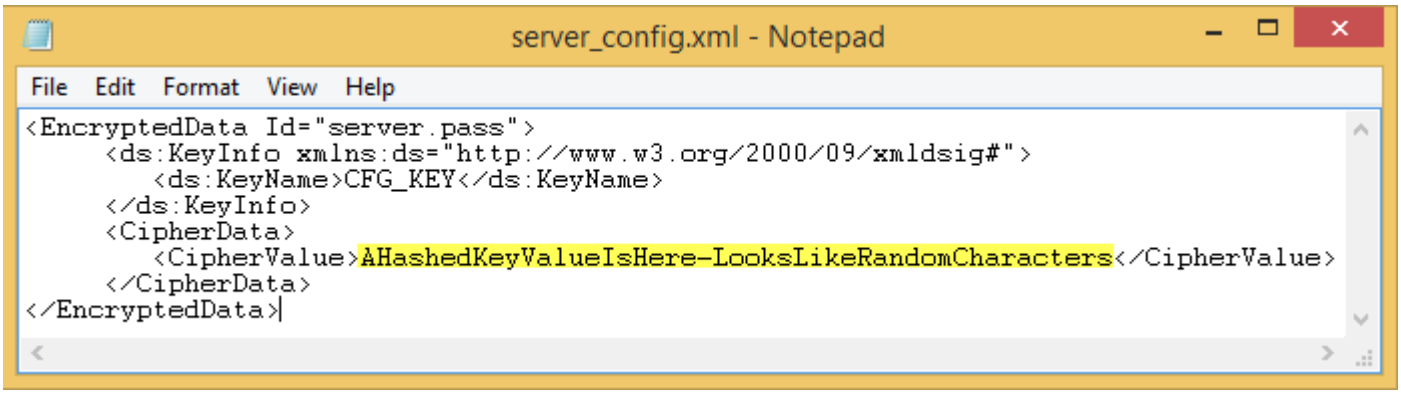
- Sitúe el valor *KeyName* de **CFG_KEY** en **ninguno.**
- Ingrese la contraseña en texto legible sin formato entre las etiquetas *<value> </value>*, que en el ejemplo corresponde a **<value>changeit</value>**
- Cuando Servidor de administración de seguridad se inicie, se cifrará la contraseña en texto legible sin formato y el valor cifrado reemplazará el valor legible.

Contraseña conocida



Si no conoce la contraseña, corte y pegue la sección similar a la sección mostrada en la Ilustración 4-2 del archivo <directorio de instalación de Compatibility Server>\conf\server_config.xml del que ha hecho copia de seguridad, en la sección correspondiente del nuevo archivo *server_config.xml*.

Contraseña desconocida



Guarde y cierre el archivo.

NOTA:
No intente cambiar la contraseña de Servidor de administración de seguridad modificando el valor server.pass en server_config.xml en ningún otro momento. Si cambia el valor en el archivo perderá el acceso a la base de datos.

Las tareas de migración del servidor back-end se completaron.

Actualización/migración de servidores front-end

NOTA: A partir de v9.5, el servicio de aviso de localización se instala como parte de esta actualización con el nombre de host predeterminado y el puerto 8446. El servicio de aviso de localización admite los avisos de devolución de llamada de Data Guardian, que insertan un aviso de devolución de llamada en cada archivo protegido por Data Guardian cuando se permiten o aplican los documentos de Office protegidos dentro del ambiente. 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.

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 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 En el cuadro de diálogo *Bienvenido*, haga clic en **Siguiente**.

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

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

El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de instalación.

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

9 Configure el servidor back-end para comunicarse con el servidor front-end.

a En el servidor back-end, vaya a <directorio de instalación de Security Server>\conf\ y abra el archivo application.properties.
b Localice publicdns.server.host y establezca el nombre en un nombre de host externamente determinable.
c Localice publicdns.server.port y establezca el puerto (el predeterminado es 8443).

Dell Services se reinicia al final de la instalación. No es necesario reiniciar Dell Server hasta que se completen las tareas de configuración posteriores a la instalación.

Instalación en el modo desconectado

El modo desconectado aísla Servidor de administración de seguridad desde Internet, de una LAN no protegida o de otras redes no protegidas. Después de instalar Servidor de administración de seguridad en Modo desconectado, permanecerá en dicho modo y no se podrá volver a cambiar a Modo conectado.

Servidor de administración de seguridad se instala en Modo desconectado desde la línea de comandos.

La siguiente tabla enumera los modificadores disponibles.

Modificador	Significado
/v	Envía las variables al archivo .msi dentro de *.exe
/s	Modo silencioso

La siguiente tabla muestra las opciones de visualización disponibles.

Opción	Significado
/q	Sin diálogo de progreso; se reinicia automáticamente tras completar el proceso
/qb	Diálogo de progreso con botón **Cancelar**
/qn	Sin interfaz de usuario

La tabla a continuación indica los parámetros disponibles para la instalación. Estos parámetros se pueden especificar en la línea de comandos o llamar desde un archivo mediante la propiedad:

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

Parámetros
AGREE_TO_LICENSE=Yes: este valor debe ser "Yes".
PRODUCT_SN=xxxxx: opcional si la información de licencia se encuentra en la ubicación estándar. De lo contrario, introdúzcala aquí.
INSTALLDIR=<ruta>: opcional.
BACKUPDIR=<ruta>: es la ruta en la que se almacenan los archivos de recuperación.

Parámetros

NOTA: La estructura de carpetas creada por el instalador durante este paso de la instalación (se muestra un ejemplo a continuación) debe permanecer inalterable.

AIRGAP=1: este valor debe ser "1" para instalar Servidor de administración de seguridad en Modo desconectado.

SSL_TYPE=n: donde n es 1 para importar un certificado existente que se compró a una entidad de certificación y 2 para crear un certificado autofirmado. El valor SSL_TYPE determina las propiedades de SSL que se requerirán.

Con SSL_TYPE=1 se requieren las siguientes:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

Con SSL_TYPE=2 se requieren las siguientes:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY: opcional, valor predeterminado= "EE. UU."

SSL_STATENAME

SSOS_TYPE=n: donde n es 1 para importar un certificado existente que se compró a una entidad de certificación y 2 para crear un certificado autofirmado. El valor SSOS_TYPE determina las propiedades de SSOS que se requerirán.

Con SSOS_TYPE=1 se requieren las siguientes:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

Con SSOS_TYPE=2 se requieren las siguientes:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY: opcional, valor predeterminado= "EE. UU."

SSOS_STATENAME

DISPLAY_SQLSERVER: este valor se analiza para obtener la información de la instancia y el puerto de SQL Server.

Ejemplo:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE: opcional. El valor predeterminado es FALSE, lo que significa que no se crea la base de datos. La base de datos ya debe existir en el servidor.

Para crear una nueva base de datos, establezca este valor en TRUE.

Parámetros

IS_SQLSERVER_AUTHENTICATION=0: opcional. El valor predeterminado es 0, lo que especifica que se utilizan las credenciales de autenticación de Windows del usuario conectado actualmente para autenticarlas en el SQL Server. Para usar la autenticación de SQL, establezca este valor en 1.

NOTA: El instalador debe autenticar el SQL Server con los siguientes permisos: crear base de datos, agregar usuario y asignar permisos. Las credenciales son credenciales del tiempo de instalación, no del tiempo de ejecución.

Si se utiliza la autenticación de SQL, se necesita lo siguiente:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION: necesario. Especifique el método de autenticación que utilizará el producto. Este paso conecta una cuenta al producto. Estas credenciales también las utilizan los servicios de Dell a medida que funcionan con Servidor de administración de seguridad. Para utilizar la autenticación de Windows, establezca este valor en 0. Para usar la autenticación de SQL, establezca el valor en 1.

NOTA: Asegúrese de que la cuenta tiene derechos de administrador del sistema y la capacidad de administrar el SQL Server. La cuenta de usuario debe tener el esquema predeterminado de permisos de SQL Server: dbo y pertenencia al rol de base de datos: dbo_owner, public.

SQL_EE_USERNAME: necesario. Con la autenticación de Windows, utilice este formato: DOMINIO\nombre de usuario. Con la autenticación de SQL, especifique el nombre de usuario.

SQL_EE_PASSWORD: necesario. Especifique la contraseña asociada al nombre de usuario de Windows o SQL.

Si se utiliza la autenticación de SQL (EE_SQLSERVER_AUTHENTICATION=1), los siguientes valores son válidos:

RUNAS_KEYSERVER_USER: establezca el nombre de usuario de Windows de "ejecutar como" de Key Server en este formato: Dominio \usuario. Debe ser una cuenta de usuario de Windows.

RUNAS_KEYSERVER_PSWD: establezca la contraseña de Windows de "ejecutar como" de Key Server asociada a la cuenta de usuario de Windows.

SQL_ADD_LOGIN=T: opcional. El valor predeterminado es nulo (no se agrega este inicio de sesión). Cuando el valor se establece en T, si el SQL_EE_USERNAME no es un inicio de sesión o usuario de la base de datos, el instalador intentará agregar las credenciales de autenticación de SQL del usuario y configurar los privilegios para permitir que el producto las utilice.

A continuación se enumeran los parámetros de nombre de host. Edite nombres de host solo si fuera necesario. Dell recomienda utilizar los valores predeterminados. El formato debe ser `server.domain.com`.

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

CORESERVERHOST: opcional. Nombre de host de Core Server.

RMIHOST: opcional. Nombre de host de Compatibility Server.

REPORTERHOST: opcional. Nombre de host de Compliance Reporter.

DEVICEHOST: opcional. Nombre de host de Device Server.

KEYSERVERHOST: opcional. Nombre de host de Key Server.

TIGAHOST: opcional. Nombre de host de Security Server.

SMTP_HOST: opcional. Nombre de host de SMTP.

ACTIVEMQHOST: opcional. Nombre de host de Message Broker.

Parámetros

A continuación se enumeran los parámetros de puertos. Edite puertos solo si fuera necesario. Dell recomienda utilizar los valores predeterminados

SERVERPORT_CLIENTAUTH: opcional.

REPORTERPORT: opcional.

DEVICEPORT: opcional.

KEYSERVERPORT: opcional.

GKPORT: opcional.

TIGAPORT: opcional.

SMTP_PORT: opcional.

ACTIVEMQ_TCP: opcional.

ACTIVEMQ_STOMP: opcional.

Instalar Servidor de administración de seguridad en Modo desconectado

En el siguiente ejemplo se instala Servidor de administración de seguridad en modo silencioso con un diálogo de progreso utilizando los parámetros de instalación que se indican en el archivo: `C:\mysetups\eeoptions.txt\" "`

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

Desinstalar Servidor de administración de seguridad

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 desinstalar Servidor 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. En el cuadro de diálogo *Bienvenido*, haga clic en **Siguiente**.
4. En el cuadro de diálogo *Quitar el programa*, haga clic en **Quitar**.
   El cuadro de diálogo de progreso muestra el estado a lo largo del proceso de desinstalación.
5. Cuando se complete la desinstalación, haga clic en **Finalizar**.

5

Configuración posterior a la instalación

Lea la asesoría técnica de *Servidor de administración de seguridad* para conocer las soluciones alternativas actuales o los problemas conocidos relacionados con la configuración de Servidor de administración de seguridad.

Ya sea que instale Servidor de administración de seguridad por primera vez o esté actualizando una instalación existente, algunos componentes de su entorno se deben configurar.

Después de instalar Servidor 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 del modo DMZ

Si Security Server se implementa en una DMZ y una red privada y solo el servidor DMZ tiene un certificado de dominio de una autoridad de certificación (CA) de confianza, serán necesarios algunos pasos manuales para agregar el certificado de confianza al almacén de claves Java del Security Server de la red privada.

Si se utiliza un certificado de confianza, omita esta sección.

NOTA: Dell recomienda encarecidamente el uso de certificados de dominio de una entidad emisora de certificados de confianza para servidores DMZ y de red privada.

Para obtener más información sobre la actualización del certificado para Dell Encryption con un certificado existente en el keystore de Microsoft, visite http://www.dell.com/support/article/us/en/19/sln297240/.

Herramienta de configuración del servidor

Cuando las configuraciones en su entorno pasan a ser necesarias después de completar su instalación, utilice la Herramienta de configuración del servidor para realizar los cambios.

La Herramienta de configuración del servidor permite:

- Agregar certificados nuevos o actualizados

- Importar certificado Dell Manager
- Importar certificado de identidad
- Configurar los valores para el Certificado Server SSL
- Configuración de los valores de SMTP para Data Guardian o los servicios de correo electrónico
- Cambiar el nombre, ubicación o credenciales de la base de datos
- Migrar la base de datos

Los programas Dell Core Server y Compatibility Server no se pueden ejecutar al mismo tiempo que la Herramienta de configuración del servidor. Detenga el servicio de Core Server y el servicio de Compatibility Server en *Servicios* (**Inicio > Ejecutar**. Escriba ***services.msc***) antes de iniciar la Herramienta de configuración del servidor.

Para iniciar la Herramienta de configuración del servidor, vaya a **Inicio** > **Dell** > **Ejecutar herramienta de configuración del servidor**.

La Herramienta de configuración del servidor lleva un registro de la actividad en **C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs.**

Agregar certificados nuevos o actualizados

Tiene la opción de elegir qué tipo de certificados utilizar (autofirmados o con firma):

- Los certificados **Autofirmados** están firmados por su propio creador. Los certificados autofirmados son adecuados para pilotos, POC, etc. Para un entorno de producción, Dell recomienda certificados con firma de entidad emisora de certificados (CA) pública o certificados con firma de dominio.
- Los certificados **Firmados** (con firma de CA pública o con firma de dominio) están firmados por una CA pública o un dominio. En caso de que los certificados estén firmados por una autoridad de certificación (CA) pública, el certificado de la CA firmante ya existirá en el almacén de certificados de Microsoft y, por lo tanto, la cadena de confianza se establece de forma automática. Para los certificados de dominio con firma de una CA, si la estación de trabajo se ha incorporado al dominio, el certificado con firma de la CA del dominio se habrá agregado al almacén de certificados de Microsoft de la estación de trabajo, de esta forma también se crea una cadena de confianza.

Los componentes que quedan afectados por la configuración del certificado son:

- Java Services (por ejemplo, Device Server y así sucesivamente)
- Aplicaciones .NET (Core Server)
- Validación de tarjetas inteligentes utilizadas para la Autenticación previa al inicio (Security Server)
- Importaciones de clave de cifrado privada para firmar paquetes de políticas enviados a Dell Manager. Dell Manager ejecuta la validación SSL para los clientes Encryption administrados con unidades de cifrado automático o BitLocker Manager.
- Estaciones de trabajo cliente:
  - Estaciones de trabajo que ejecutan BitLocker Manager
  - Estaciones de trabajo que ejecutan Encryption Enterprise (Windows)
  - Estaciones de trabajo que ejecutan Endpoint Security Suite Enterprise

Información relativa a qué tipo de certificado utilizar:

La Autenticación previa al inicio mediante tarjetas inteligentes requiere validación SSL con Security Server. Dell Manager realiza la validación SSL cuando se conecta a Dell Core Server. Para estos tipos de conexiones, la CA firmante deberá estar en el keystore (ya sea en el keystore de Java o en el keystore de Microsoft, según el componente de Dell Server que se esté tratando). Si se eligen certificados autofirmados, las siguientes opciones están disponibles:

- Validación de tarjetas inteligentes utilizadas para la Autenticación previa al inicio:
  - Importe el certificado con firma de “Agencia raíz” y la cadena de confianza completa al almacén de claves de Java de Security Server. Se debe importar la cadena de confianza completa.

Dell Manager:

- Ingrese el certificado con firma de “Agencia raíz” (desde el certificado autofirmado generado) en las “Entidades de certificación raíz de confianza” (para “equipo local”) de la estación de trabajo en el keystore de Microsoft.
- Modifique el comportamiento de la validación SSL del lado servidor. Para desactivar la validación de confianza SSL del lado del servidor, seleccione **Deshabilitar comprobación de cadena de confianza** en la pestaña Configuración.

Existen dos métodos para crear un certificado: *Exprés* y *Avanzado*.

Seleccione **un** método:

- Exprés: seleccione este método para generar un certificado autofirmado para todos los componentes. Este es el método más sencillo, pero los certificados autofirmados son adecuados solo para pilotos, POC, etc. Para un entorno de producción, Dell recomienda certificados con firma de entidad emisora de certificados (CA) pública o certificados con firma de dominio.
- Advanced: seleccione este método para configurar cada uno de los componentes por separado.

Exprés

1 En el menú superior, seleccione **Acciones** > **Configurar certificados**.

2 Cuando se inicie el Asistente de configuración, seleccione **Exprés** y haga clic en **Siguiente**. Se utiliza la información del certificado autofirmado que se creó al instalar Servidor de administración de seguridad si está disponible.

3 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

La configuración del certificado ha finalizado. El resto de este apartado detalla el método avanzado para crear un certificado.

Avanzado

Existen dos rutas para crear un certificado: *Generar un certificado autofirmado* y *Utilizar la configuración actual*. Seleccione **una** ruta:

- Ruta 1: Generar un certificado de autofirma
- Ruta 2: Utilizar la configuración actual

Ruta 1: Generar un certificado de autofirma

1 En el menú superior, seleccione **Acciones** > **Configurar certificados**.

2 Cuando se inicie el Asistente de configuración, seleccione **Avanzado** y haga clic en **Siguiente**.

3 Seleccione **Generar certificado autofirmado** y haga clic en **Siguiente**. Se utiliza la información del certificado autofirmado que se creó al instalar Servidor de administración de seguridad si está disponible.

4 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

La configuración del certificado ha finalizado. El resto de este apartado detalla el otro método avanzado para crear un certificado.

Ruta 2: Utilizar la configuración actual

1 En el menú superior, seleccione **Acciones** > **Configurar certificados**.

2 Cuando se inicie el Asistente de configuración, seleccione **Avanzado** y haga clic en **Siguiente**.

3 Seleccione **Utilizar configuración actual** y haga clic en **Siguiente**.

4 En la ventana *Certificado SSL del Compatibility Server*, seleccione **Generar certificado autofirmado** y haga clic en **Siguiente**. Se utiliza la información del certificado autofirmado que se creó al instalar Servidor de administración de seguridad si está disponible.

   Haga clic en **Siguiente**.

5 En la ventana *Certificado SSL de Core Server*, seleccione una de las siguientes opciones:

   - *Seleccionar certificado*: seleccione esta opción para utilizar un certificado existente. Haga clic en **Siguiente**.

     Navegue hasta la ubicación del certificado existente, ingrese la contraseña asociada con el certificado existente y haga clic en **Siguiente**.

Haga clic en **Finalizar** cuando haya terminado.

- *Generar certificado autofirmado*: se utiliza la información del certificado autofirmado que se creó al instalar Servidor de administración de seguridad si está disponible. Si selecciona esta opción, la ventana de Certificado de Message Security no se mostrará (la ventana sí aparece si selecciona la opción *Utilizar configuración actual*) y se utiliza el certificado creado para Dell Compatibility Server.

  Compruebe que el nombre de equipo completo (FQDN) sea correcto. Haga clic en **Siguiente**.

  Se mostrará un mensaje de aviso que indica que ya existe un certificado con el mismo nombre. Cuando le pregunte si desea utilizarlo, haga clic en **Sí**.

  Haga clic en **Finalizar** cuando haya terminado.
- *Utilizar configuración actual*: seleccione esta opción para cambiar un valor de un certificado en cualquier momento después de la configuración inicial de Servidor de administración de seguridad. Si se selecciona esta opción, el certificado previamente configurado permanece en su lugar. Cuando seleccione esta opción, aparecerá la ventana de certificado de Message Security.

  En el certificado de Message Security, seleccione **una** de las siguientes opciones:

  – *Seleccionar certificado*: seleccione esta opción para utilizar un certificado existente. Haga clic en **Siguiente**.

    Navegue hasta la ubicación del certificado existente, ingrese la contraseña asociada con el certificado existente y haga clic en **Siguiente**.

    Haga clic en **Finalizar** cuando haya terminado.

  – *Generar certificado autofirmado*: se utiliza la información del certificado autofirmado que se creó al instalar Servidor de administración de seguridad si está disponible.

    Haga clic en **Siguiente**.

    Haga clic en **Finalizar** cuando haya terminado.

La configuración del certificado ha finalizado.

Cuando se completen los cambios:

1. En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.
2. Cierre la Herramienta de configuración de Dell Server.
3. Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

Importar certificado Dell Manager

Si su implementación incluye clientes Servidor de administración de seguridad administrados remotamente con agentes de administración de cifrado, debe importar su certificado creado recientemente (o existente). El certificado Dell Manager se utiliza como medio para proteger la clave privada utilizada para firmar los paquetes de políticas enviados a clientes Servidor de administración de seguridad administrados remotamente y al agente de administración de cifrado. Este certificado puede ser independiente de cualquiera de los otros certificados. Además, si esta clave perdió su carácter confidencial, puede sustituirse por una nueva y Dell Manager solicitará una nueva clave pública si no puede descifrar los paquetes de políticas.

1. Abra Microsoft Management Console.
2. Haga clic en **Archivo** > **Agregar o quitar complemento**.
3. Haga clic en **Agregar**.
4. En la ventana *Agregar complemento autónomo*, seleccione **Certificados** y haga clic en **Agregar**.
5. Seleccione **Cuenta de equipo** y haga clic en **Siguiente**.

6 En la ventana *Seleccionar equipo*, seleccione **Equipo local (el equipo en el que se ejecuta esta consola)** y haga clic en **Finalizar**.

7 Haga clic en **Cerrar**.

8 Haga clic en **Aceptar**.

9 En la carpeta *Raíz de consola*, expanda *Certificados (equipo local)*.

10 Vaya a la carpeta *Personal* y busque el certificado deseado.

11 Resalte el certificado deseado y haga clic con el botón derecho del mouse en **Todas las tareas** > **Exportar**.

12 Cuando se abra el asistente para exportación de certificados, haga clic en **Siguiente**.

13 Seleccione **Sí, exportar la clave privada** y haga clic en **Siguiente**.

14 Seleccione **Intercambio de información personal - PKCS #12 (.PFX)** y, a continuación, seleccione las subopciones **Incluir todos los certificados en la ruta de certificación (si es posible)** y **Exportar todas las propiedades extendidas**. Haga clic en **Siguiente**.

15 Ingrese y confirme una contraseña. Puede elegir la contraseña que desee. Elija una contraseña que recuerde fácilmente, pero que los demás no puedan saber. Haga clic en **Siguiente**.

16 Haga clic en **Examinar** para ir a la ubicación en la que desea guardar el archivo.

17 En *Nombre de archivo*, ingrese un nombre para guardar el archivo como. Haga clic en **Guardar**.

18 Haga clic en **Siguiente**.

19 Haga clic en **Finalizar**.

20 Aparecerá un mensaje que indica que la exportación se ha realizado con éxito. Cierre el MMC.

21 Vuelva a la Herramienta de configuración de Dell Server.

22 En el menú superior, seleccione **Acciones** > **Importar certificado DM**.

23 Vaya a la ubicación donde se guardaron los archivos exportados. Seleccione el archivo y haga clic en **Abrir**.

24 Ingrese la contraseña asociada a este archivo y haga clic en **Aceptar**.

La importación del certificado Dell Manager habrá ahora finalizado.

Cuando se completen los cambios:

1 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

2 Cierre la Herramienta de configuración de Dell Server.

3 Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

Importar certificado BETA de SSL/TLS

Si su implementación incluye Server Encryption, deberá importar el certificado recién creado (o existente). El certificado BETA SSL/TLS protege la clave privada utilizada para firmar los paquetes de políticas que se envían a servidores cliente.

1 En el menú superior, seleccione **Acciones** > **Importar certificado BETA SSL/TLS**.

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

3 En el indicador de *Contraseña de certificado*, ingrese la contraseña asociada con el certificado existente.

4 En el Diálogo de cuenta de Windows, seleccione una opción:

   a Para cambiar las credenciales asociadas con el certificado de identidad, seleccione **Utilizar credenciales de cuenta de Windows diferentes con el certificado de identidad.**

   b Para continuar utilizando las credenciales de la cuenta que ha iniciado sesión, haga clic en **Siguiente**.

5 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

Configurar los valores para el Certificado Server SSL

En la Herramienta de configuración del servidor, haga clic en la pestaña **Configuración**.

Dell Manager:

Para desactivar la validación de confianza SSL del lado del servidor de Dell Manager, seleccione **Deshabilitar comprobación de cadena de confianza**.

SCEP:

Si utiliza Mobile Edition, ingrese la URL del servidor que aloja SCEP.

NOTA: A partir de v9.8, ya no se admite Mobile Edition.

Cuando se completen los cambios:

1 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

2 Cierre la Herramienta de configuración de Dell Server.

3 Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

Configurar valores de SMTP

En la Herramienta de configuración del servidor, haga clic en la pestaña **SMTP**.

Esta pestaña configura los valores SMTP para Data Guardian, boletines de productos, notificaciones y mensajes de transmisión de amenazas de Advanced Threat Prevention.

Cuando se hayan finalizado de realizar los cambios a la configuración, reinicie el servicio del Servidor de seguridad. Para que se actualicen las configuraciones, se debe reiniciar el servicio del Servidor de seguridad.

Ingrese la siguiente información:

1 En *Nombre de host*, ingrese el FQDN de su servidor SMTP, por ejemplo, nombreservidorsmtp.dominio.com.

2 En *Nombre de usuario*, ingrese el nombre de usuario para iniciar sesión en el servidor de correo. El formato puede ser DOMINIO \jperez, jperez, o el formato que requiera su organización.

3 En *Contraseña*, ingrese la contraseña asociada con este nombre de usuario.

4 En *Dirección de remitente*, ingrese la dirección de correo electrónico desde la que se originará el correo electrónico. Esta puede coincidir con la cuenta para el nombre de usuario (jperez@dominio.com), pero también puede ser otra cuenta diferente a la que dicho usuario tenga acceso para enviar mensajes en su nombre (registroenlanube@dominio.com).

5 En *Puerto*, ingrese el número de puerto (normalmente 25).

6 En el menú *Autenticación*, seleccione *Verdadero* o *Falso*.

NOTA: El nombre de usuario y la contraseña se deben dejar en blanco si la autenticación está establecida en falso.

Cuando se completen los cambios:

1 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

2 Cierre la Herramienta de configuración de Dell Server.

3 Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

Cambiar el nombre, ubicación o credenciales de la base de datos

En la herramienta de configuración del servidor, haga clic en la pestaña **Base de datos**.

1 En *Nombre del servidor*, ingrese el nombre de dominio completo (si hay un nombre de la instancia, inclúyalo), del servidor que aloja la base de datos. Por ejemplo, SQLTest.domain.com\DellDB.

   Dell recomienda utilizar un nombre de dominio completo, a pesar de que también puede usarse una dirección IP.

2 En *Puerto del servidor*, ingrese el número de puerto.

   Al utilizar una instancia de SQL Server no predeterminada, debe especificar el puerto dinámico de la instancia en *Puerto:*. Como alternativa, habilite el servicio SQL Server Browser y asegúrese de que el puerto UDP 1434 esté abierto. Para obtener más información, consulte https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

3 En *Base de datos*, ingrese el nombre de la base de datos.

4 En *Autenticación:*, seleccione **Autenticación de Windows** o **Autenticación de SQL Server**. Si selecciona la autenticación de Windows, se utilizan las mismas credenciales que se usaron para iniciar sesión en Windows (*Nombre de usuario* y *Contraseña* no se pueden editar).

5 En *Nombre de usuario:*, ingrese el nombre de usuario correspondiente asociado con esta base de datos.

6 En *Contraseña:*, ingrese la contraseña para el nombre de usuario que aparece en *Nombre de usuario*.

7 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

8 Para probar la configuración de la base de datos, en el menú superior, seleccione **Acciones > Probar configuración de base de datos**. Se inicia el asistente de configuración.

9 En la ventana *Probar configuración* , lea la información de la prueba y haga clic en **Siguiente**.

10 Si selecciona la autenticación de Windows en la pestaña *Base de datos*, puede, como opción, ingresar credenciales alternativas para permitir el uso de las mismas credenciales que se utilizan para ejecutar Servidor de administración de seguridad. Haga clic en **Siguiente**.

11 En la ventana *Probar configuración* se mostrarán la resultados de Probar configuración de conexión, Prueba de compatibilidad y Prueba de migración de la base de datos.

12 Haga clic en **Finalizar**.

NOTA:

Si la base de datos SQL o la instancia SQL está configurada con una intercalación no predeterminada, la intercalación no predeterminada debe distinguir mayúsculas de minúsculas. Para obtener una lista de intercalaciones y distinciones de mayúsculas y minúsculas, consulte https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Cuando se completen los cambios:

1 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

2 Cierre la Herramienta de configuración de Dell Server.

3 Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

Migrar la base de datos

Puede migrar una base de datos v9.2 o posterior al esquema más reciente con la actualización más reciente del servidor.

En la herramienta de configuración del servidor, haga clic en la pestaña **Base de datos**.

1 Si todavía no ha realizado una copia de seguridad de su base de datos de Dell Server existente, **hágalo ahora**.

2 En el menú superior, seleccione **Acciones > Migrar base de datos**. Se inicia el asistente de configuración.

3 En la ventana *Migrar base de datos de Enterprise* se mostrará un aviso. Confirme que haya hecho una copia de seguridad de toda la base de datos, o confirme que no sea necesario hacer una copia de seguridad de la base de datos existente. Haga clic en **Siguiente**.

   En la ventana *Migrar base de datos*, mensajes informativos mostrarán el estado de la migración.

   Al finalizar, compruebe que no existan errores.

   NOTA: Un mensaje de error identificado por  indica que ha habido un error en una tarea de la base de datos y que debe tomarse una acción correctiva para poder migrar correctamente la base de datos. Haga clic en Finalizar, corrija los errores de la base de datos y reinicie las instrucciones de este apartado.

4 Haga clic en **Finalizar**.

Cuando finalice la migración:

1 En el menú superior, seleccione **Configuración** > **Guardar**. Si se le pide, confirme que desea guardar.

2 Cierre la Herramienta de configuración de Dell Server.

3 Haga clic en **Inicio** > **Ejecutar**. Escriba *services.msc* y haga clic en **Aceptar**. Cuando se abra *Servicios*, navegue hasta cada Dell Service y haga clic en **Iniciar el servicio**.

6

Tareas administrativas

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 e inicie sesión con las credenciales de usuario del dominio.

Cargar licencia de acceso de cliente

Debe recibir las licencias de acceso de cliente aparte de los archivos de instalación, ya sea en la compra inicial o posteriormente al agregar licencias de acceso de cliente adicionales.

1 En el panel izquierdo, haga clic en **Administración**.

2 Haga clic en **Administración de licencias**.

3 Haga clic en **Seleccionar archivo** para encontrar y seleccionar el archivo de la Licencia del cliente.

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**.

Configurar Dell Compliance Reporter

1 En el panel izquierdo, haga clic en **Compliance Reporter**.
2 Cuando se inicie Dell Compliance Reporter, inicie sesión utilizando las credenciales predeterminadas de *superadmin/changeit*.

Realizar copias de seguridad

Para fines de recuperación ante desastres, asegúrese de que se realice una copia de seguridad de las siguientes ubicaciones semanalmente, con diferenciales cada noche. Para obtener más información acerca de la planificación de recuperación ante desastres, consulte http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en. Para obtener más información acerca del respaldo de los datos de Compliance Reporter, consulte http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en.

Copias de seguridad de Servidor de administración de seguridad

Realice periódicamente una copia de seguridad de los archivos almacenados en la ubicación seleccionada para las copias de seguridad de los archivos de configuración durante la instalación (paso 10 en la página 27) o la actualización/migración (paso 6 en la página 68). Se admiten copias de seguridad semanales de estos datos, ya que cambiaría poco y se puede volver a configurar manualmente si fuera necesario. Los archivos más críticos almacenan información necesaria para conectarse a la base de datos:

<carpeta de instalación>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<carpeta de instalación>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<carpeta de instalación>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

Copias de seguridad de SQL Server

Realice copias de seguridad completas todas las noches con registros transaccionales habilitados, así como copias de seguridad de bases de datos diferenciales cada 3-4 horas. Si una base de datos de copia de seguridad está disponible, entonces la recomendación es que se realicen las tareas de envío de registros o registros de transacciones en intervalos de 15 minutos (si es posible, más cortos). Al igual que en otros casos, Dell aconseja el uso de las prácticas recomendadas para la base de datos de Dell Server y que se incluya el software Dell en el plan de recuperación ante desastres de su organización.

Para obtener información adicional sobre las prácticas recomendadas de SQL Server, consulte la siguiente lista, dichas prácticas deben implementarse cuando se instale Dell Security si no se han implementado aún.

Copias de seguridad de PostgreSQL Server

Los eventos de auditoría se almacenan en el servidor PostgreSQL, del que se debería realizar una copia de seguridad con regularidad. Para obtener instrucciones sobre cómo realizar las copias de seguridad, consulte https://www.postgresql.org/docs/9.5/static/backup.html.

Dell recomienda el uso de las prácticas recomendadas para la base de datos de PostgreSQL y que se incluya el software Dell en el plan de recuperación tras desastres de su organización.

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	HTTP(S)/ 8443	Consola de administración y centro de control para implementación en toda la empresa.
Core Server	HTTPS/ 8888	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.
Device Server	HTTPS/ 8081	Permite activaciones y la recuperación de la contraseña. Un componente de Servidor de administración de seguridad. Se necesita para Encryption Enterprise (Windows y Mac)
Security Server	HTTPS/ 8443	Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, Data Guardian, la comunicación de SED-PBA y Active Directory para la autenticación o la reconciliación, incluida la validación de identidades para la autenticación en la consola de administración. Requiere el acceso de base de datos SQL.
Compatibility Server	TCP/ 1099	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 y STOMP/ 61613	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. Requiere el acceso de base de datos SQL.
Key Server	TCP/ 8050	Negocia, autentica y cifra una conexión cliente utilizando las API de Kerberos.

Nombre	Puerto predeterminado	Descripción
		Requiere acceso a la base de datos SQL para extraer los datos clave.
Policy Proxy	TCP/ 8000	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario.
PostGres	TCP/ 5432	Base de datos local utilizada para los datos de eventos.
LDAP	TCP/ 389/636 (controladora de dominio local), 3268/3269 (catálogo global) TCP/ 135/ 49125+ (RPC)	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.
Base de datos de Microsoft SQL	TCP/ 1433	El puerto de SQL Server predeterminado es 1433 y se asignan a los puertos clientes un valor aleatorio entre 1024 y 5000.
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	Permite insertar un aviso de devolución de llamada en cada archivo de Office protegidos, al ejecutar Data Guardian en el modo de Office protegido.

8

Prácticas recomendadas para SQL Server

La siguiente lista explica las prácticas recomendadas para el SQL Server, que deben implementarse cuando se instale Dell Security si no se han implementado aún.

1 Asegúrese de que el tamaño del bloque NFTS donde residen el archivo de registro y el de datos es de 64 KB. Las extensiones de SQL Server (unidad básica de SQL Storage) son de 64 KB.

   Para obtener más información, busque en los artículos de Microsoft TechNet para encontrar "Understanding Pages and Extents" (Comprensión de las páginas y extensiones).

   - Microsoft SQL Server 2008 R2: http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 Como pauta general, establezca una cantidad de memoria máxima para el SQL Server del 80 por ciento de la memoria instalada.

   Para obtener más información, busque en los artículos de Microsoft TechNet para encontrar *Server Memory Server Configuration Options* (Opciones de configuración del servidor de la memoria del servidor).

   - Microsoft SQL Server 2008 R2: http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
   - Microsoft SQL Server 2012: https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014: https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016: https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017: https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3 Establezca -t1222 en las propiedades de inicio de la instancia para asegurar que se captura la información de interbloqueo si se produce uno.

   Para obtener más información, busque en los artículos de Microsoft TechNet para encontrar "Trace Flags (Transact-SQL)" (Marcador de seguimiento [Transact-SQL]).

   - Microsoft SQL Server 2008 R2: http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
   - Microsoft SQL Server 2012: https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014: https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016: https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017: https://msdn.microsoft.com/en-us/library/ms188396.aspx

4 Asegúrese de que se cubren todos los índices con una tarea de mantenimiento semanal para reconstruirlos.

9

Certificados

En este capítulo se explica cómo obtener certificados para su uso con Servidor de administración de seguridad.

Para obtener información sobre cómo configurar la autenticación de SmartCard, consulte http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en

Para obtener información sobre los requisitos mínimos para solicitar los certificados SSL/TLS para que los utilice el Dell Data Security server, consulte http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en

Para obtener más información sobre la actualización del certificado para Dell Encryption con un certificado existente en el keystore de Microsoft, visite http://www.dell.com/support/article/us/en/19/sln297240/.

Creación de un certificado autofirmado y generación de una solicitud de firma de certificado

Esta sección explica los pasos necesarios para crear un certificado autofirmado para componentes basados en Java. Este proceso **no puede** utilizarse para crear un certificado autofirmado en componentes basados en .NET.

Dell *solamente* recomienda los certificados autofirmados en un entorno que no sea de producción.

Si su organización exige un certificado de servidor SSL, o si necesita crear un certificado por cualquier otro motivo, esta sección describe el proceso de creación de un keystore de java utilizando la herramienta Keytool.

Si su organización tiene pensado utilizar tarjetas inteligentes para la autenticación, debe utilizar Keytool para importar la cadena de certificados completos de confianza que se utilizan en el certificado del usuario de tarjetas inteligentes.

Keytool crea claves privadas que se transmiten en un formato de Solicitud de firma de certificado (CSR) a una Autoridad de certificación (CA), como puede ser VeriSign® o Entrust®. La CA, basada en esta CSR, crea y firma un certificado de servidor. El certificado de servidor se descarga entonces a un archivo, junto con el certificado de la autoridad de firma. Los certificados se importan a continuación al archivo cacerts.

Generación de un nuevo par de claves y un certificado autofirmado

1 Navegue hasta el directorio **conf** de Compliance Reporter, Security Server o Device Server.

2 Realice una copia de seguridad de la base de datos de certificados predeterminada:

Haga clic en **Inicio** > **Ejecutar** e ingrese `move cacerts cacerts.old`.

3 Agregue Keytool a la ruta del sistema. Escriba el siguiente comando en la línea de comandos:

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 Para generar un certificado, ejecute Keytool como se muestra:

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Ingrese la siguiente información cuando Keytool se la solicite.

> **NOTA:**
> Haga una copia de seguridad de los archivos de configuración antes de modificarlos. Cambie únicamente los parámetros especificados. Si se cambia algún otro dato de estos archivos, incluso las etiquetas, el sistema podría dañarse y presentar errores. Dell no puede garantizar que los problemas derivados de modificaciones no autorizadas a estos archivos se puedan resolver sin reinstalar Servidor de administración de seguridad.

- *Contraseña de Keystore*: escriba una contraseña (los caracteres no compatibles son <>;&" '), y establezca la variable en el archivo **conf** del componente en el mismo valor, tal como sigue:

  <Directorio de instalación de Compliance Reporter>\conf\eserver.properties. Establezca el valor eserver.keystore.password =

  <Directorio de instalación de Device Server>\conf\application.properties. Establezca el valor keystore.password =

  <Directorio de instalación de Security Server>\conf\application.properties. Establezca el valor keystore.password =
- *Nombre completo del servidor*: escriba el nombre completo del servidor en el que esté instalado el componente con el que esté trabajando. Este nombre de dominio completo incluye el nombre de host y el nombre de dominio (por ejemplo: servidor.dominio.com).
- *Unidad organizacional*: ingrese el valor adecuado (ejemplo: Seguridad).
- Organización: ingrese el valor correspondiente (por ejemplo, Dell).
- *Ciudad o localidad*: ingrese el valor adecuado (ejemplo: Dallas).
- *Estado o provincia*: ingrese el nombre de la provincia o el estado sin abreviar (por ejemplo: Texas).
- código de dos letras del país.
- La utilidad solicita la confirmación de que la información es correcta. Si fuera así, escriba `yes`.

  Si no, escriba `no`. Keytool muestra cada valor ingresado previamente. Haga clic en **Intro** para aceptar el valor o cambie el valor y haga clic en **Intro**.
- *Contraseña de clave para alias*: si no se ingresa otra contraseña aquí, esta contraseña predetermina a la contraseña de clasificación de claves.

Solicitud de certificado firmado a una Autoridad de certificación

Utilice este procedimiento para generar una Solicitud de firma de certificado (CSR) para el certificado autofirmado creado en Generación de un nuevo par de claves y un certificado autofirmado.

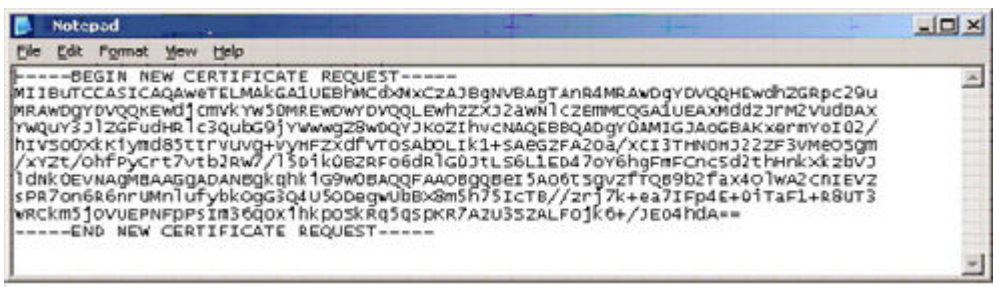
1 Sustituya el mismo valor utilizado anteriormente para <**certificatealias**>:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

Por ejemplo, `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

El archivo .csr contiene un par PRINCIPIO/FIN que se utiliza durante la creación del certificado por parte de la CA.

Archivo .CSR de ejemplo



2 Siga el proceso de su organización para la adquisición de un certificado de servidor SSL de una autoridad de certificación. Envíe el contenido de <csr-filename> para su firma.

> **NOTA:**
> Hay varios métodos para solicitar un certificado válido. Se muestra un método de ejemplo en **Método de ejemplo para solicitar un certificado**.

3 Cuando reciba el certificado firmado, guárdelo en un archivo.

4 La práctica recomendada es realizar una copia de seguridad de este certificado, en caso de que ocurra un error durante el proceso de importación. Este respaldo evita tener que comenzar todo el proceso otra vez.

Importación de un certificado raíz

Si la autoridad de certificación del certificado raíz es Verisign (no Verisign Test), pase al siguiente procedimiento e importe el certificado firmado.

El certificado raíz de la autoridad de certificación valida los certificados firmados.

1 Realice **uno** de los siguientes pasos:

- Descargue el certificado raíz de la autoridad de certificación y guárdelo en un archivo.
- Obtenga el certificado raíz del servidor de directorios empresarial.

2 Realice **uno** de los siguientes pasos:

- Si habilita SSL para Compliance Reporter, Security Server o Device Server, cambie al directorio **conf** del componente.
- Si habilita SSL entre Servidor de administración de seguridad y el servidor de directorio empresarial, cambie a <**directorio de instalación de Dell>\Java Runtimes\jre1.x.x_xx\lib\security** (la contraseña predeterminada para el cacerts JRE es **changeit**).

3 Ejecute Keytool de la siguiente manera para instalar el certificado raíz:

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

Por ejemplo, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Método de ejemplo para solicitar un certificado

Un ejemplo de un método para solicitar un certificado es utilizar un navegador web a fin de acceder al servidor de CA de Microsoft que su organización habría configurado internamente.

1 Navegue hasta el servidor de CA de Microsoft. Su organización le proporciona la dirección IP.

2 Seleccione **Solicitar un certificado** y haga clic en **Siguiente**.

Servicios de certificado de Microsoft

3 Seleccione **Solicitud avanzada** y haga clic en **Siguiente**.

Elegir tipo de solicitud

4 Seleccione la opción para **Enviar una solicitud de certificado mediante el archivo PKCS #10 de codificación base64** y haga clic en **Siguiente**.

Solicitud de certificado avanzado

5 Pegue el contenido de la solicitud CSR en el cuadro de texto. Seleccione una plantilla de certificado de **Web Server** y haga clic en **Enviar**.

Enviar una solicitud guardada

6 Guarde el certificado. Seleccione **DER codificado** y haga clic en **Descargar certificado de CA**.

Descargar certificado de CA

7 Guarde el certificado. Seleccione **DER codificado** y haga clic en **Descargar ruta de certificación CA**.

Descargar ruta de acceso del certificado de CA

8 Importe el certificado de la autoridad de firma convertido. Volver al símbolo del sistema. Escriba:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Ahora que ya ha importado el certificado de la autoridad de firma, puede importar el certificado del servidor (puede establecerse la cadena de confianza). Escriba:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Utilice el alias del certificado autofirmado para emparejar la solicitud de CSR con el certificado del servidor.

10 La entrada del archivo cacerts muestra que el certificado del servidor tiene una **longitud de cadena de certificado** de **2**, lo que indica que el certificado no está autofirmado. Escriba:

```
keytool -list -v -keystore cacerts
```

La huella digital del segundo certificado en la cadena es el certificado importado de la autoridad de certificación (que también aparece en el listado bajo el certificado del servidor en la lista).

Exportación de un certificado a .PFX mediante la Consola de administración de certificados

Después de tener un certificado en formato de archivo .crt en MMC, deberá convertirlo en un archivo .pfx para su uso con Keytool cuando Security Server se utilice en el modo DMZ *y* al importar un certificado de Dell Manager a la Herramienta de configuración del servidor.

1 Abra Microsoft Management Console.
2 Haga clic en **Archivo** > **Agregar o quitar complemento**.
3 Haga clic en **Agregar**.
4 En la ventana *Agregar complemento autónomo*, seleccione **Certificados** y haga clic en **Agregar**.
5 Seleccione **Cuenta de equipo** y haga clic en **Siguiente**.
6 En la ventana *Seleccionar equipo*, seleccione **Equipo local (el equipo en el que se ejecuta esta consola)** y haga clic en **Finalizar**.
7 Haga clic en **Cerrar**.
8 Haga clic en **Aceptar**.
9 En la carpeta *Raíz de consola*, expanda *Certificados (equipo local)*.
10 Vaya a la carpeta *Personal* y busque el certificado deseado.
11 Resalte el certificado deseado y haga clic con el botón derecho del mouse en **Todas las tareas** > **Exportar**.
12 Cuando se abra el asistente para exportación de certificados, haga clic en **Siguiente**.
13 Seleccione **Sí, exportar la clave privada** y haga clic en **Siguiente**.
14 Seleccione **Intercambio de información personal - PKCS #12 (.PFX)** y, a continuación, seleccione las subopciones **Incluir todos los certificados en la ruta de certificación (si es posible)** y **Exportar todas las propiedades extendidas**. Haga clic en **Siguiente**.
15 Ingrese y confirme una contraseña. Puede elegir la contraseña que desee. Elija una contraseña que recuerde fácilmente, pero que los demás no puedan saber. Haga clic en **Siguiente**.
16 Haga clic en **Examinar** para ir a la ubicación en la que desea guardar el archivo.

17 En *Nombre de archivo*, ingrese un nombre para guardar el archivo como. Haga clic en **Guardar**.

18 Haga clic en **Siguiente**.

19 Haga clic en **Finalizar**.

Aparecerá un mensaje que indica que la exportación se ha realizado con éxito. Cierre el MMC.

Cómo agregar un certificado de firma de confianza a Security Server cuando se ha utilizado un certificado no de confianza para SSL

1 Detenga el servicio de Security Server si se está ejecutando.

2 Realice copia de seguridad del archivo cacerts en <directorio de instalación de Security Server>\conf\.

Utilice Keytool para hacer lo siguiente:

3 Exporte el PFX de confianza a un archivo de texto y documente el alias:

```
keytool -list -v -keystore "
```

4 Importe el PFX al archivo cacerts de <directorio de instalación de Security Server>\conf\.

```
keytool -importkeystore -v -srckeystore "
```

5 Modifique el valor keystore.alias.signing de <directorio de instalación de Security Server>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

Inicie el servicio de Security Server.