

Dell Data Protection

Enterprise Server Installation and Migration Guide (Guía de instalación y migración de Enterprise Server) v9.7



ⓘ | NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

⚠ | PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

⚠ | AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

© 2017 Dell Inc. Todos los derechos reservados. Dell, EMC, y otras marcas comerciales son marcas comerciales de Dell Inc. o de sus filiales. Puede que otras marcas comerciales sean marcas comerciales de sus respectivos propietarios.

Marcas comerciales y marcas comerciales registradas utilizadas en el conjunto de documentos de Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise y Dell Data Guardian: Dell™ y el logotipo de Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® y KACE™ son marcas comerciales de Dell Inc. Cylance®, CylancePROTECT y el logotipo de Cylance son marcas comerciales registradas de Cylance, Inc. en los EE. UU. y en otros países. McAfee McAfee® y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, Inc. en los Estados Unidos y en otros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® y Xeon® son marcas comerciales registradas de Intel Corporation en los EE. UU. y en otros países. Adobe®, Acrobat®, y Flash® son marcas comerciales registradas de Adobe Systems Incorporated. Authen Tec® y Eikon® son marcas comerciales registradas de Authen Tec. AMD® es una marca comercial registrada de Advanced Micro Devices, Inc. Microsoft®, Windows® y Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® y Visual C++® son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y otros países. VMware® es una marca comercial o una marca comercial registrada de VMware, Inc. en Estados Unidos o en otros países. Box® es una marca comercial registrada de Box. DropboxSM es una marca de servicio de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® y Google™ Play son marcas comerciales o marcas comerciales registradas de Google Inc. en los Estados Unidos y en otros países. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud@SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® y Siri® son marcas de servicio, marcas comerciales o marcas comerciales registradas de Apple, Inc. en los Estados Unidos y/o en otros países. GO ID®, RSA® y SecurID® son marcas comerciales registradas de Dell EMC. EnCase™ y Guidance Software® son marcas comerciales o marcas comerciales registradas de Guidance Software. Entrust® es una marca comercial registrada de Entrust®, Inc. en Estados Unidos y otros países. InstallShield® es una marca comercial registrada de Flexera Software en Estados Unidos, China, Unión Europea, Hong Kong, Japón, Taiwán y Reino Unido. Micron® y RealSSD® son marcas comerciales registradas de Micron Technology, Inc. en Estados Unidos y otros países. Mozilla® Firefox® es una marca comercial registrada de Mozilla Foundation en los Estados Unidos y/o en otros países. iOS® es una marca comercial o una marca comercial registrada de Cisco Systems, Inc. en los Estados Unidos y en determinados países y se utiliza bajo licencia. Oracle® y Java® son marcas comerciales registradas de Oracle y/o sus filiales. Los demás nombres utilizados pueden ser marcas comerciales de sus respectivos propietarios. SAMSUNG™ es una marca comercial de SAMSUNG en los Estados Unidos o en otros países. Seagate® es una marca comercial registrada de Seagate Technology LLC en Estados Unidos y otros países. Travelstar® es una marca comercial registrada de HGST, Inc. en Estados Unidos y otros países. UNIX® es una marca comercial registrada de The Open Group. VALIDITY™ es una marca comercial de Validity Sensors, Inc. en los Estados Unidos y en otros países. VeriSign® y otras marcas relacionadas son las marcas comerciales o marcas comerciales registradas de VeriSign, Inc. o sus afiliados o filiales en los Estados Unidos y en otros países y han otorgado la licencia a Symantec Corporation. KVM on IP® es una marca comercial registrada de Video Products. Yahoo!® es una marca comercial registrada de Yahoo! Inc. Este producto utiliza partes del programa 7-Zip. El código fuente se puede encontrar en 7-zip.org. Con licencia GNU LGPL + restricciones de unRAR (7-zip.org/license.txt).

Enterprise Server Installation and Migration Guide (Guía de instalación y migración de Enterprise Server)

2017 - 04

Rev. A01

Tabla de contenido

1 Introducción a Dell Enterprise Server.....	5
Acerca de Dell Enterprise Server.....	5
Cómo ponerse en contacto con Dell ProSupport.....	5
2 Requisitos y arquitectura de Dell Enterprise Server.....	6
Requisitos de Dell Enterprise Server.....	6
Requisitos previos de Dell Enterprise Server.....	6
Hardware de Dell Enterprise Server.....	6
Software de Dell Enterprise Server.....	7
Compatibilidad de idiomas en Dell Enterprise Server.....	9
Diseño de arquitectura de Dell Enterprise Server.....	10
3 Configuración previa a la instalación.....	15
Configuración.....	15
4 Instalación o actualización/migración.....	21
Antes de comenzar la instalación o la actualización/migración.....	21
Nueva instalación.....	22
Instalación del servidor back-end y una base de datos nueva.....	22
Instalación del servidor back-end con base de datos existente.....	26
Instalación del servidor front-end.....	30
Actualización/migración.....	32
Antes de comenzar la actualización/migración.....	32
Actualización/migración de servidores back-end.....	34
Actualización/migración de servidores front-end.....	36
Instalación en el modo desconectado.....	37
Instalación de Enterprise Server en modo desconectado.....	40
Desinstalación de Dell Enterprise Server.....	40
5 Configuración posterior a la instalación.....	41
Instalación y configuración de EAS Management.....	41
Instalar EAS Device Manager.....	41
Instalar EAS Mailbox Manager.....	42
Utilizar EAS Configuration Utility.....	42
Configuración de los valores de administración de EAS.....	43
Configuración de Dell Security Server en modo DMZ.....	43
Utilizar Keytool para importar el certificado de dominio DMZ.....	43
Modificar el archivo application.properties.....	44
Inscripción a APN.....	44
Herramienta de configuración del servidor.....	45
Agregar certificados nuevos o actualizados.....	45
Importar certificado Dell Manager.....	48
Importar certificado de identidad.....	49



Configurar los valores para el Certificado Server SSL o Mobile Edition.....	49
Configuración de los valores de SMTP para Data Guardian o los servicios de correo electrónico.....	50
Cambiar el nombre, ubicación o credenciales de la base de datos.....	50
Migrar la base de datos.....	51
6 Tareas administrativas.....	52
Asignar rol de administrador Dell.....	52
Iniciar sesión con rol de administrador Dell.....	52
Cargar licencia de acceso de cliente.....	52
Confirmar políticas.....	52
Configurar Dell Compliance Reporter.....	53
Configurar autenticación SQL con Compliance Reporter.....	53
Configurar autenticación Windows con Compliance Reporter.....	53
Realizar copias de seguridad.....	54
Copias de seguridad de Enterprise Server.....	54
Copias de seguridad de SQL Server.....	54
Copias de seguridad de PostgreSQL Server.....	54
7 Descripciones de los componentes Dell.....	55
8 Prácticas recomendadas para SQL Server.....	58
9 Certificados.....	59
Creación de un certificado autofirmado y generación de una solicitud de firma de certificado.....	59
Generación de un nuevo par de claves y un certificado autofirmado.....	59
Solicitud de certificado firmado a una Autoridad de certificación.....	60
Importación de un certificado raíz.....	61
Método de ejemplo para solicitar un certificado.....	61
Exportación de un certificado a .PFX mediante la Consola de administración de certificados.....	62
Cómo agregar un certificado de firma de confianza a Security Server cuando se ha utilizado un certificado no de confianza para SSL.....	63



Introducción a Dell Enterprise Server

Acerca de Dell Enterprise Server

Enterprise Server es la parte de administración de la seguridad de la solución de Dell. Remote Management Console permite a los administradores supervisar el estado de los extremos, el cumplimiento de políticas y la protección en toda la empresa.

Enterprise Server tiene las siguientes características:

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

Cómo ponerse en contacto con Dell ProSupport

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

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

Asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado teniendo su Código de servicio disponible cuando realice la llamada.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte [Números de teléfono internacionales de Dell ProSupport](#).



Requisitos y arquitectura de Dell Enterprise Server

Esta sección describe los requisitos de hardware y software y las recomendaciones de diseño de la arquitectura para la implementación de Dell Data Protection.

Requisitos de Dell Enterprise Server

Los componentes de Dell Enterprise Server tienen requisitos de hardware y software además del software proporcionado en el medio de instalación de Dell. Asegúrese de que el entorno de instalación satisfaga dichos requisitos antes de seguir con las tareas de instalación o actualización/migración.

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

Requisitos previos de Dell Enterprise Server

La siguiente tabla detalla el software que debe estar instalado antes de instalar Dell Enterprise Server. Los enlaces e instrucciones para instalar estos requisitos previos se detallan en [Configuración previa a la instalación](#).

Cada elemento de software aplicable debe instalarse antes de comenzar la instalación, a menos que se indique que el instalador instala el elemento. De lo contrario, la instalación fallará.

Hardware de Dell Enterprise Server

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.

Requisitos previos

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

La siguiente tabla detalla los requisitos *mínimos* de hardware para Dell Enterprise Server. Consulte [Diseño de arquitectura de Dell Enterprise Server](#) para obtener más información acerca de la expansión basada en el tamaño de su implementación.

Requisitos de Hardware

Procesador

CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

CPU moderna de cuatro núcleos (2 GHz+) para una configuración de servidor único

RAM

8 GB mínimo, dependiendo de la configuración

16 GB para una configuración de servidor único

Espacio libre en disco

Alrededor de 1,5 GB de espacio de disco libre (más el espacio para el archivo de paginación)

20 GB o más de espacio de disco libre (más el espacio de paginación virtual) para una configuración de servidor único

Tarjeta de red

Tarjeta de interfaz de red de 10/100/1000

Varios

TCP/IPv4 instalado y activado

Software de Dell Enterprise Server

La siguiente tabla detalla los requisitos de software para Dell Enterprise Server y Proxy Server.

ⓘ NOTA: Se debe deshabilitar UAC antes de la instalación. El servidor debe reiniciarse para que el cambio tenga efecto. En Windows Server 2012 R2 y Windows Server 2016, el instalador desactiva UAC.

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

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

Dell Enterprise Server - Servidor back-end y servidor front-end

- **Windows Server 2008 R2 SP0 - SP1 (64 bits)**

- Standard Edition

- Enterprise Edition

- **Windows Server 2008 SP2 (64 bits)**

- Standard Edition

- Enterprise Edition



- **Windows Server 2012 R2**

- Standard Edition
- Datacenter Edition

- **Windows Server 2016**

- Standard Edition
- Datacenter Edition

Servidores Exchange ActiveSync

Si tiene pensado utilizar Mobile Edition, se ofrece compatibilidad con los siguientes servidores Exchange ActiveSync. Este componente se instala en el Exchange Server front-end.

- Exchange ActiveSync 12.0: un componente de Exchange Server 2007
- Exchange ActiveSync 12.1: un componente de Exchange Server 2007 SP1
- Exchange ActiveSync 14.0: un componente de Exchange Server 2010
- Exchange ActiveSync 14.1: un componente de Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) debe instalarse/configurarse en Exchange Server.

Repositorio LDAP

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

Entornos virtuales recomendados para los componentes Dell Enterprise Server

Dell Enterprise Server se puede instalar opcionalmente en un entorno virtual. Solo se recomiendan los siguientes entornos.

Dell Enterprise Server v9.7 se ha validado con Hyper-V Server (instalación completa o básica) y como rol en Windows Server 2012 R2 o Windows Server 2016.

- Hyper-V Server (instalación completa o básica)
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo
 - 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
 - Para obtener más información, consulte <https://technet.microsoft.com/en-us/library/hh923062.aspx>.

Dell Enterprise Server v9.7 se ha validado con VMware ESXi 5.5 y VMware ESXi 6.0. Asegúrese de que todos los parches y actualizaciones se apliquen inmediatamente a VMware ESXi para abordar las posibles vulnerabilidades.

① | NOTA: Cuando se ejecutan VMware ESXi y Windows Server 2012 R2 o Windows Server 2016, 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



- No es necesario un sistema operativo
- Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
- El hardware debe cumplir con los requisitos mínimos de VMWare
- 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
- Para obtener más información, consulte <http://pubs.vmware.com/vsphere-55/index.jsp>.
- VMWare ESXi 6.0
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo
 - Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Consulte <http://pubs.vmware.com/vsphere-60/index.jsp> para obtener más información.

NOTA: La base de datos de SQL Server que aloje el Dell Enterprise Server debe estar ejecutándose en un equipo independiente.

Base de datos

- **SQL Server 2008 y SQL Server 2008 R2** Standard Edition / Enterprise Edition
- **SQL Server 2008 SP4 (con KB3045311)** 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

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.

Remote Management Console de Dell Data Protection 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.

Compatibilidad de idiomas en Dell Enterprise Server

Remote Management Console es compatible con la Interfaz de usuario multilingüe (MUI) y admite los idiomas siguientes.

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)	



Diseño de arquitectura de Dell Enterprise Server

Las soluciones Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise y Data Guardian son productos extremadamente escalables, escalados en el tamaño de su organización y en el número de extremos seleccionados para el cifrado. Esta sección proporciona un conjunto de pautas para escalar la arquitectura para 5000 a 60 000 extremos.

NOTA: Si la organización tiene más de 50 000 extremos, póngase en contacto con Dell ProSupport para recibir ayuda.

NOTA:

Cada uno de los componentes enumerados en cada sección incluye las especificaciones de hardware mínimas, que se necesitan para asegurar un rendimiento óptimo en la mayoría de los entornos. No distribuir los recursos adecuados a cualquiera de estos componentes puede resultar en una degradación de rendimiento o problemas funcionales con la aplicación.

Hasta 5000 extremos

Esta arquitectura admite la mayoría de negocios de tamaño pequeño y mediano que tienen entre 1 y 5000 extremos. Todos los componentes de Dell Enterprise Server se pueden instalar en un servidor individual. De manera opcional, el servidor front-end se puede colocar en el DMZ para publicar políticas y/o activar extremos en Internet.

Componentes de la arquitectura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Configuración de servidor único

16 GB: 20 GB o más de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos (2 GHz+)

Configuración de servidor cuando se utiliza con servidores front-end

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

Servidor front-end externo de Dell

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 y SQL Server 2008 SP4 (con KB3045311) 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

5000 - 20 000 extremos

Esta arquitectura admite entornos que tengan entre 5000 y 20 000 extremos. Se agrega un servidor front-end para distribuir la carga adicional y está diseñado para administrar aproximadamente 15 000 - 20 000 extremos. De manera opcional, el servidor front-end se puede colocar en el DMZ para publicar políticas y/o activar extremos en Internet.

Componentes de la arquitectura

Dell Enterprise Server

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

Servidor front-end interno de Dell (1) y servidor front-end externo de Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 y SQL Server 2008 SP4 (con KB3045311) 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

20 000 - 40 000 extremos

Esta arquitectura admite entornos que tengan entre 20 000 y 40 000 extremos. Se agrega un servidor front-end adicional para distribuir la carga adicional. Cada front-end adicional está diseñado para administrar aproximadamente 15 000 - 20 000 extremos. De manera opcional, el servidor front-end se puede colocar en el DMZ para publicar políticas y/o activar extremos en Internet.

Componentes de la arquitectura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

Servidores front-end internos de Dell (2) y servidor front-end externo de Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition



Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 y SQL Server 2008 SP4 (con KB3045311) 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

40 000 - 60 000 extremos

Esta arquitectura admite entornos que tengan entre 40 000 y 60 000 extremos. Se agrega un servidor front-end adicional para distribuir la carga adicional. Cada front-end adicional está diseñado para administrar aproximadamente 15 000 - 20 000 extremos. De manera opcional, el servidor front-end se puede colocar en el DMZ para publicar políticas y/o activar extremos en Internet.

NOTA:

Si la organización tiene más de 50 000 extremos, póngase en contacto con Dell ProSupport para recibir ayuda.

Componentes de la arquitectura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

Servidores front-end internos de Dell (2) y servidor front-end externo de Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits Standard o Enterprise Edition

Windows Server 2012 R2 Standard o Datacenter Edition

Windows Server 2016 Standard o Datacenter Edition

Mínimo 8 GB, dependiendo de la configuración; +-1,5 GB de espacio de disco libre (más el espacio de paginación virtual); CPU moderna de cuatro núcleos mínimo (2 GHz+), incluidos Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o equivalente AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 y SQL Server 2008 SP4 (con KB3045311) 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

Consideraciones de alta disponibilidad

Esta arquitectura representa una arquitectura altamente disponible que admite hasta 60 000 extremos. Hay dos Dell Enterprise Servers configurados en una configuración activa/pasiva. Para conmutar por error el segundo Dell Enterprise Server, detenga los servicios en el nodo principal y que el alias DNS (CNAME) señale al nodo secundario. Inicie los servicios en el segundo nodo e inicie la Remote Management Console para asegurar que la aplicación esté funcionando correctamente. Los servicios en el segundo nodo (pasivo) deben configurarse como "Manual" para prevenir que dichos servicios se inicien por accidente durante la revisión o el mantenimiento.

Una organización también puede decidir tener un servidor de base de datos del clúster SQL. En esta configuración, Dell Enterprise Server debe estar configurado para utilizar el nombre de host o la IP del clúster.

NOTA:

No se admite la replicación de la base de datos.

El tráfico de cliente se distribuye a lo largo de tres servidores front-end internos. De manera opcional, varios servidores front-end se pueden colocar en el DMZ para publicar políticas y/o activar extremos en Internet.

Virtualización

Dell Enterprise Server se puede instalar opcionalmente en un entorno virtual. Solo se recomiendan los siguientes entornos.

Dell Enterprise Server v9.7 se ha validado con Hyper-V Server (instalación completa o básica) y como rol en Windows Server 2012 R2 o Windows Server 2016.

- Hyper-V Server (instalación completa o básica)
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo
 - 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
 - Para obtener más información, consulte <https://technet.microsoft.com/en-us/library/hh923062.aspx>.

Dell Enterprise Server v9.7 se ha validado con VMware ESXi 5.5 y VMware ESXi 6.0. Asegúrese de que todos los parches y actualizaciones se apliquen inmediatamente a VMware ESXi para abordar las posibles vulnerabilidades.

NOTA: Cuando se ejecutan VMware ESXi y Windows Server 2012 R2 o Windows Server 2016, 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
 - No es necesario un sistema operativo
 - Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Para obtener más información, consulte <http://pubs.vmware.com/vsphere-55/index.jsp>.
- VMWare ESXi 6.0
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo



- Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
- El hardware debe cumplir con los requisitos mínimos de VMWare
- 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
- Consulte <http://pubs.vmware.com/vsphere-60/index.jsp> para obtener más información.

ⓘ | NOTA: La base de datos de SQL Server que aloje el Dell Enterprise Server debe estar ejecutándose en un equipo independiente.

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.

Las tareas de mantenimiento de la base de datos deben incluir la reconstrucción de todos los índices de la base de datos y la recopilación de estadísticas.

Configuración previa a la instalación

Antes de empezar, lea las *Enterprise Server Technical Advisories* (Asesorías técnicas de Enterprise Server) para ver cualquiera de las soluciones alternativas o los problemas conocidos relacionados con Dell Enterprise Server.

La configuración previa a la instalación del servidor o los servidores en los que tiene pensado instalar Dell Enterprise Server es muy importante. Preste especial atención a este apartado para garantizar una instalación fluida de Dell Enterprise Server.

Configuración

- 1 Si está habilitado, desactive Configuración de seguridad mejorada (ESC) de Internet Explorer. Agregue la URL del servidor a los sitios de confianza en las opciones de seguridad el explorador. 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 Dell Policy Proxy externa a Dell Message Broker: TCP/61616 y STOMP/61613

Comunicación con el back-end de Dell Security Server: HTTPS/8443

Comunicación con el back-end de Dell Core Server: HTTPS/8888 y 9000

Comunicación con los puertos RMI - 1099

Comunicación con el back-end de Dell Device Server: HTTP(S)/8443: si su Dell Enterprise Server es v 7.7 o posterior. Si su Dell Enterprise 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 SQL: TCP/1433

Remote Management Console: HTTPS/8443

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

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084 (configurado automáticamente en la instalación)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 y 9000 (8888 se configura automáticamente en la instalación)



Dell Device Server: HTTP(S)/8443 (Dell Enterprise Server v7.7 o posterior) o HTTP(S)/8081 (pre-v.7.7 Dell Enterprise Server)

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell 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

NOTA:

Si sus clientes Enterprise Edition estarán autorizados de fábrica o si usted compra las licencias de fábrica, siga estas instrucciones para configurar GPO en la controladora de dominio para habilitar los derechos (es posible que no sea el servidor que ejecuta Enterprise Edition). Asegúrese de que el puerto de salida 443 esté disponible para establecer comunicación con el servidor. Si el puerto 443 está bloqueado por cualquier motivo, la función de autorización no funcionará. Para obtener más información, consulte la [Enterprise Edition Advanced Installation Guide](#) (Guía de instalación avanzada de Enterprise Edition).

Creación de una base de datos Dell

- 3 Si aún no tuviera configurada una base de datos SQL para Dell Enterprise Server, el instalador creará la base de datos por usted durante la instalación. Si prefiere configurar una base de datos antes de instalar Dell Enterprise Server, siga las instrucciones que se indican a continuación para crear la base de datos SQL y el usuario SQL en SQL Management Studio. ***Estas instrucciones son opcionales, ya que el instalador creará una base de datos para el usuario si no hay una ya.***

Cuando instale Dell Enterprise Server, siga las instrucciones de [instalar servidor de back-end con la base de datos existente](#).

Enterprise Server está preparado tanto para la autenticación SQL como para la de Windows. El método de autenticación predeterminado es la autenticación 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 Dell Enterprise Server, 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](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx).

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](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx).

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

Creación de una nueva base de datos de Windows SQL Server mediante la autenticación de Windows:

- a Haga clic en **Inicio > Todos los programas > Microsoft SQL Server > Management Studio**.
- b Haga clic con el botón derecho en la carpeta Bases de datos y, a continuación, haga clic en Nueva base de datos. Se mostrará el cuadro de diálogo Propiedades de la base de datos.
- c Introduzca el nombre de la base de datos y haga clic en **Aceptar**.
- d Expanda la carpeta *Seguridad* y haga clic con el botón derecho en **Inicios de sesión**.
- e Haga clic en **Nuevo inicio de sesión** para crear un propietario para la nueva base de datos.
- f Introduzca un nombre de usuario en el campo *Nombre*.

- g Seleccione la opción de autenticación *Autenticación de Windows*.
- h Seleccione **Asignación de usuarios** y, a continuación, resalte la nueva base de datos.
- i Seleccione el rol de base de datos (db_owner) y haga clic en **Aceptar**.

O bien

Creación de una nueva base de datos de SQL Server con la autenticación de SQL Server:

- a Haga clic en **Inicio > Todos los programas > Microsoft SQL Server > Management Studio**.
- b Haga clic con el botón derecho en la carpeta *Bases de datos* y, a continuación, haga clic en **Nueva base de datos**. Se mostrará el cuadro de diálogo *Propiedades de la base de datos*.
- c Introduzca el nombre de la base de datos y haga clic en **Aceptar**.
- d Expanda la carpeta *Seguridad* y haga clic con el botón derecho en **Inicios de sesión**.
- e Haga clic en **Nuevo inicio de sesión** para crear un propietario para la nueva base de datos.
- f Introduzca un nombre de usuario en el campo *Nombre*.
- g Seleccione la opción de autenticación *Autenticación de SQL Server*. Introduzca y confirme la contraseña.
- h Deseleccione **Exigir caducidad de contraseña**.
- i Seleccione **Asignación de usuarios** y, a continuación, resalte la nueva base de datos.
- j Seleccione el rol de base de datos (db_owner) y haga clic en **Aceptar**.

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 Dell Enterprise Server instale estos componentes.

Windows Server 2008 y Windows Server 2008 R2 - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555>

Instalar .NET Framework 4.5

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

Windows Server 2008 y Windows Server 2008 R2 - <https://www.microsoft.com/en-us/download/details.aspx?id=42643>

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 Dell Enterprise Server instale este componente.

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

Configurar Microsoft CA (MSCEP)

Este paso solo debe realizarse en el servidor que ejecute MSCEP si tiene pensado utilizar iOS con Mobile Edition.

- 7 Configure MSCEP.

Windows Server 2008 R2 debe ser Enterprise Edition. **Con Standard Edition no se puede instalar el rol MSCEP.**

- a Abra Server Manager. En el menú izquierdo, seleccione **Funciones de servidor** y active la casilla para **Servicios de certificados de Active Directory**. Haga clic en **Siguiente**. El asistente para agregar roles le llevará a los siguientes pasos.

En *AD CS > Servicios de función*, active las casillas para los servicios de rol **Entidad de certificación** e **Inscripción web de entidad de certificación**. Seleccione **Agregar servicios de función necesarios para el servidor web IIS** (si se le solicita). Haga clic en **Siguiente**.

En *AD CS > Tipo de configuración*, seleccione **Autónoma**. Haga clic en **Siguiente**.

En *AD CS > Tipo de CA*, seleccione **CA subordinada**. Haga clic en **Siguiente**.



En *AD CS > Clave privada*, seleccione **Crear una nueva clave privada**. Haga clic en **Siguiente**.

En *AD CS > Clave privada > Criptografía*, mantenga los valores predeterminados de **RSA#Proveedor de almacenamiento de claves de software de Microsoft, 2048** y **SHA1**. Haga clic en **Siguiente**.

En *AD CS > Clave privada > Nombre de CA*, mantenga todos los valores predeterminados. Haga clic en **Siguiente**.

En *AD CS > Clave privada > Solicitud de certificado*, seleccione **Enviar una solicitud de certificado a una CA primaria**. Seleccione **Examinar por: nombre de CA**. Busque y seleccione **CA primaria**. Haga clic en **Siguiente**.

En *AD CS > Base de datos de certificados*, mantenga los valores predeterminados. Haga clic en **Siguiente**.

En *Servidor web (IIS)*, haga clic en **Siguiente**.

En *Servidor web (IIS) > Servicios de función*, mantenga los valores predeterminados. Haga clic en **Siguiente**.

En *Confirmación*, haga clic en **Instalar**.

En *Resultados*, revise los resultados y haga clic en **Cerrar**.

En *Administrador de servidores > Funciones*, seleccione **Agregar servicios de función** en *Servicios de certificados de Active Directory*.

Cuando aparezca la ventana *Seleccionar servicios de función*, active la casilla para **Servicio de inscripción de dispositivos de red**. Haga clic en **Siguiente**.

Agregue la cuenta de usuario que el *Servicio de inscripción de dispositivos de red* debe utilizar al autorizar solicitudes de certificado al grupo de usuarios de IIS_IUSRS del servidor local. El formato es dominio\nombre de usuario. Haga clic en **Aceptar**.

En la ventana *Especificar cuenta de usuario*, seleccione el usuario que acaba de agregar al grupo IIS_IUSRS. Haga clic en **Siguiente**.

En la ventana *Especificar información de entidad de registro*, mantenga los valores predeterminados para *Información requerida* y *Agregar información opcional* según sea necesario. Haga clic en **Siguiente**.

En la ventana *Configurar criptografía para entidad de registro*, mantenga los valores predeterminados. Haga clic en **Siguiente**.

En la ventana *Confirmar selecciones de instalación*, haga clic en **Instalar**.

En la ventana *Resultados de la instalación*, revise los resultados y haga clic en **Cerrar**.

Cierre el Administrador del servidor.

- b Modifique la clave de registro de esta forma:

```
HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
```

```
"EnforcePassword"=dword:00000000
```

- c Abra IIS Manager. Explore en profundidad en `\<ServerName> \Sites\Default Web Site\CertSrv\mscep_admin..`

Abra *Autenticación* y habilite **Autenticación anónima**.

- d Haga clic en **Inicio > Ejecutar**. Escriba `certsrv.msc` y haga clic en **Intro**.

Cuando aparezca la ventana `certsrv`, haga clic con el botón derecho en el nombre del servidor, seleccione **Propiedades** y haga clic en la pestaña **Módulo de políticas**.

Haga clic en **Propiedades** y seleccione **Seguir la configuración de la plantilla de certificados si es aplicable. De otra manera, emitir siempre el certificado automáticamente**. Haga clic en **Aceptar**.

- e Cierre IIS Manager.

- f Reinicie el servidor. Para comprobarlo, abra Internet Explorer y en la barra de direcciones, introduzca `http://servidor.dominio.com/certsrv/mscep_admin/`

Finalización de la configuración de MSCEP Windows Server 2008 R2.

Windows Server 2012 R2 o Windows Server 2016:

- a Siga las Instrucciones de configuración en el artículo, [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#). (Servicio de inscripción de dispositivos de red [NDES] en los Servicios de certificados de Active Directory).

- b Modifique la clave de registro de esta forma:

```
HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
```

```
"EnforcePassword"=dword:00000000
```

- c Abra IIS Manager. Explore en profundidad `\<ServerName\Sites\Default Web Site\CertSrv\mscep_admin`.

Abra *Autenticación* y habilite **Autenticación anónima**.

- d Haga clic en **Inicio > Ejecutar**. Escriba `certsrv.msc` y haga clic en **Intro**.

Cuando aparezca la ventana `certsrv`, haga clic con el botón derecho en el nombre del servidor, seleccione **Propiedades** y haga clic en la pestaña **Módulo de políticas**.

Haga clic en **Propiedades** y seleccione **Seguir la configuración de la plantilla de certificados si es aplicable. De otra manera, emitir siempre el certificado automáticamente**. Haga clic en **Aceptar**.

- e Cierre IIS Manager.

- f Reinicie el servidor. Para comprobarlo, abra Internet Explorer y en la barra de direcciones, introduzca

```
http://servidor.dominio.com/certsrv/mscep_admin/
```

Finalización de la configuración de MSCEP Windows Server 2012 R2/Windows Server 2016.

Instalación/configuración de Microsoft Message Queuing (MSMQ)

Este paso solo debe realizarse si tiene pensado utilizar Mobile Edition. Este es un requisito previo para que EAS Device Manager y EAS Mailbox Manager puedan comunicarse.

- 8 En Windows Server 2008 o Windows Server 2008 R2 (en el servidor que aloja el entorno de Exchange): <http://msdn.microsoft.com/en-us/library/aa967729.aspx>

O bien

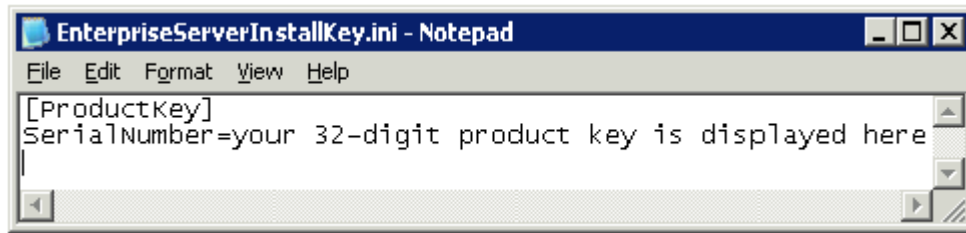
En Windows Server 2012 R2:

- a Abra Server Manager.
- b Vaya a **Administrar > Agregar roles y características**.
- c En la pantalla Antes de comenzar, haga clic en **Siguiente**.
- d Seleccione **Instalación basada en características o en roles**, y haga clic en **Siguiente**.
- e Seleccione el servidor en el que desea instalar la característica, y haga clic en **Siguiente**.
- f No seleccione roles de servidor. Haga clic en **Siguiente**.
- g En Características, seleccione **Message Queuing** y haga clic en **Instalar**.

Opcional

- 9 **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 Dell Enterprise Server.





La configuración previa a la instalación del servidor ha finalizado. Continúe en [Instalar o actualizar/migrar](#).

Instalación o actualización/migración

Este capítulo proporciona instrucciones para realizar lo siguiente:

- **Nueva instalación:** para instalar un nuevo Dell Enterprise Server.
- **Actualización/migración:** para actualizar desde un Dell Enterprise Server v8.0 o posterior existente y funcional.
- **Desinstalación de Dell Enterprise Server:** para eliminar la instalación actual, si es necesario.

Si su instalación debe incluir más de un servidor principal (back-end), póngase en contacto 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 *Enterprise Server Technical Advisories* (Asesorías técnicas de Enterprise Server) para ver las soluciones alternativas actuales o los problemas conocidos relacionados con la instalación de Dell Enterprise Server.

Si está habilitado el Control de cuentas de usuario (UAC), debe deshabilitarlo. En Windows Server 2012 R2, el instalador deshabilita UAC. 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. Si selecciona Autenticación de Windows, se utilizarán las credenciales del usuario que ha iniciado sesión. El usuario debe tener derechos de administrador del sistema y derechos para crear y administrar la base de datos de SQL (crear base de datos, agregar usuario y asignar permisos). Para la Autenticación de SQL, la cuenta utilizada deberá tener los mismos derechos. Estas credenciales se utilizan solo durante la instalación. El producto instalado no utiliza estas credenciales.

También durante la instalación, las credenciales de autenticación de tiempo de ejecución del servicio se deben especificar para los servicios de Dell para acceder al 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: db_owner, public.

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

Dell recomienda el uso de las prácticas recomendadas para la base de datos Dell y que se incluya el software Dell en el plan de recuperación tras 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 sería instalar el servidor back-end antes de instalar y configurar el servidor front-end.

Los archivos de registro de instalación están ubicados en este directorio: **C:\ProgramData\Dell\Dell Data Protection\Installer Logs**



Nueva instalación

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

- **Instalación del servidor back-end y una base de datos nueva:** para instalar un nuevo Dell Enterprise Server y una nueva base de datos.
- **Instalación del servidor back-end con base de datos existente:** para instalar un nuevo Dell Enterprise Server 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 Dell Enterprise Server que se va a instalar. Se debe migrar una base de datos v8.x 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-v8.0, póngase en contacto con Dell ProSupport para obtener asistencia.

NOTA:

Si tiene un Dell Enterprise Server v8.x o una versión posterior que funcione, consulte las instrucciones en [Actualización/migración de servidores back-end](#).

Si instala un servidor front-end, realice esta instalación después de instalar el servidor back-end:

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

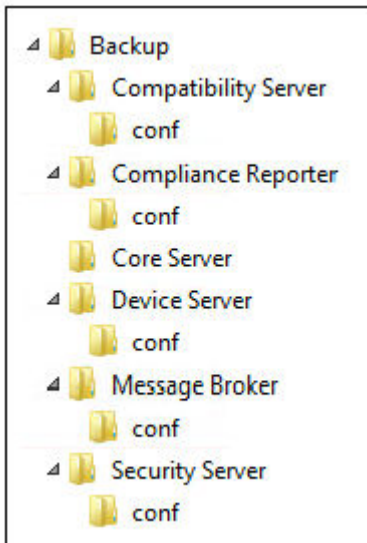
Instalación del servidor back-end y una base de datos nueva

- 1 En el medio de instalación de Dell, navegue hasta el directorio de Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a instalar Enterprise Server. **Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.**
- 2 Haga doble clic en **setup.exe**.
- 3 En el cuadro de diálogo *Asistente InstallShield*, seleccione el idioma para la instalación y, a continuación, 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 ha completado el [paso 9](#) opcional en [Configuración previa a la instalación](#), haga clic en **Siguiente**. En caso contrario, introduzca 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 Dell Enterprise Server 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 servidor.

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 introducir la ruta al certificado.

Introduzca 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*, introduzca 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 caduca en un año de manera predeterminada.

- 12 Para Server Encryption (SE), 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 introducir la ruta al certificado.

Introduzca 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*, introduzca 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 caduca en un año 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 front-end, seleccione **Trabaja con front-end para comunicarse con clientes internamente en su red o externamente en la DMZ** e introduzca el nombre de host del Servidor de seguridad 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 utilizará el instalador para configurar la base de datos Dell Data Protection. Tras la instalación, el producto instalado no utiliza las credenciales que se especifican aquí.

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

Si selecciona Autenticación de Windows, se utilizarán para la autenticación las mismas credenciales que se utilizaron para iniciar sesión en Windows (no se podrá modificar el contenido de los campos Nombre de usuario ni Contraseña). 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:
Introduzca 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**, introduzca 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 son también las utilizadas por los servicios de Dell a medida que trabajen con Dell Enterprise Server.

O bien

- **Autenticación SQL Server**

Seleccione **Autenticación del SQL Server mediante las siguientes credenciales**, introduzca las credenciales de SQL Server que utilizarán los servicios de Dell a medida que trabajen con Dell Enterprise Server 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 el servidor.

Instalación del servidor back-end con base de datos existente

NOTA:

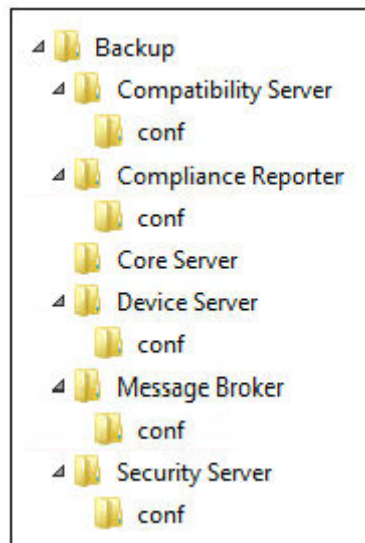
Si tiene un Dell Enterprise Server v8.x o una versión posterior que funcione, consulte las instrucciones en [Actualización/migración de servidores back-end](#).

Puede instalar un nuevo Dell Enterprise Server 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 Dell Enterprise Server que se va a instalar.

Se debe migrar una base de datos v8.x 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-v8.0**, póngase en contacto con Dell ProSupport para obtener asistencia.

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 de datos que los confirme antes de iniciar la instalación.

Si la base de datos existente se ha instalado previamente con Dell Enterprise Server, 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 está instalando Dell Enterprise Server. Acceda a estos archivos en caso necesario para configurar Dell Enterprise Server 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.



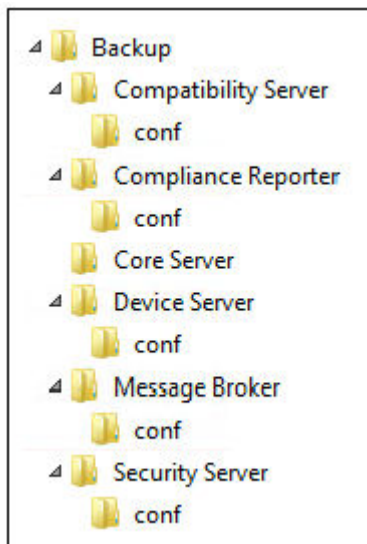
- 1 En el medio de instalación de Dell, navegue hasta el directorio de Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a instalar Enterprise Server. **Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.**
- 2 Haga doble clic en **setup.exe**.
- 3 En el cuadro de diálogo *Asistente InstallShield*, seleccione el idioma para la instalación y, a continuación, 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 ha completado el [paso 9](#) opcional en [Configuración previa a la instalación](#), haga clic en **Siguiente**. En caso contrario, introduzca 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 Dell Enterprise Server 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 servidor.

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 introducir la ruta al certificado.

Introduzca 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*, introduzca 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 caduca en un año de manera predeterminada.

- 12 Para Server Encryption (SE), 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 introducir la ruta al certificado.

Introduzca 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*, introduzca 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 caduca en un año 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 front-end, seleccione **Trabaja con front-end para comunicarse con clientes internamente en su red o externamente en la DMZ** e introduzca el nombre de host del Servidor de seguridad 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 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 Autenticación de Windows, se utilizarán para la autenticación las mismas credenciales que se utilizaron para iniciar sesión en Windows (no se podrá modificar el contenido de los campos Nombre de usuario ni Contraseña). 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**.
- 15 Seleccione el método de autenticación que utilizará el producto. Esta es la cuenta que utiliza el producto para trabajar con la base de datos y con Dell services.
- **Para utilizar la autenticación de Windows**
- Seleccione **Autenticación Windows mediante las credenciales siguientes**, introduzca 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**, introduzca 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.

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 Enterprise Server y, a continuación, ejecutar el instalador más reciente para actualizar.
 - La opción **Continuar sin migrar la base de datos** instala los archivos de Enterprise Server 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 Dell Enterprise Server, se considera una *Recuperación*. Se muestra 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**.

- 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 han completado.

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 ofrece una opción de front-end (modo DMZ) para su uso con Dell Enterprise Server. Si desea implementar componentes Dell en la DMZ, asegúrese de que estén protegidos apropiadamente frente a ataques.

NOTA: El servicio de aviso de localización se instala como parte de esta instalación para admitir 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 ejecuta en modo de Office protegido. Esto permite la comunicación entre cualquier dispositivo en cualquier ubicación y el servidor front-end de Dell. Asegúrese de que se ha configurado la seguridad de la red necesaria antes de utilizar el aviso de devolución de llamada. La política Habilitar aviso de devolución de llamada está activada de manera predeterminada.

Para realizar esta instalación, necesitará el nombre de host completo del servidor DMZ.

- 1 En el medio de instalación de Dell, navegue hasta el directorio de Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a instalar Enterprise Server. **Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.**
- 2 Haga doble clic en **setup.exe**.
- 3 En el cuadro de diálogo *Asistente InstallShield*, seleccione el idioma para la instalación y, a continuación, 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 Introduzca la Clave del producto.
- 8 Seleccione **Instalación de front-end** y haga clic en **Siguiente**.
- 9 Para instalar el servidor front-end 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 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 introducir la ruta al certificado.

Introduzca 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*, introduzca 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 caduca en un año de manera predeterminada.

- 11 En el cuadro de diálogo *Configuración del servidor front-end*, introduzca el nombre de host completo o alias de DNS del servidor back-end, seleccione **Enterprise Edition** 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 guión bajo ("_").

Deseleccione un proxy solo si estuviera seguro de que no desea configurarlo para la instalación. Si deseleccionara 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 a Dell Enterprise Server v8.0 y posteriormente a Dell Enterprise Server v9.x. Si su versión de servidor fuera anterior a v8.0, primero debe actualizar a v8.0 y posteriormente a v9.x.

Antes de comenzar la actualización/migración

Antes de comenzar, asegúrese de que se haya completado toda la [Configuración previa a la instalación](#). Es un punto de especial importancia si va a realizar la implementación de Mobile Edition.

Lea las *Enterprise Server Technical Advisories* (Asesorías técnicas de Enterprise Server) para ver las soluciones alternativas actuales o los problemas conocidos relacionados con la instalación de Dell Enterprise Server.

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 de datos que los confirme antes de iniciar la instalación.

Dell recomienda el uso de las prácticas recomendadas para la base de datos Dell y que se incluya el software Dell en el plan de recuperación tras 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 capacidades de las políticas, le recomendamos actualizar a las versiones más recientes tanto de Dell Enterprise Server como de los clientes.

Dell Enterprise Server v9.x admite:

- Enterprise Edition:
 - 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 v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Actualización/migración desde Dell Enterprise Server v8.x o posterior. (Cuando migre desde Dell Enterprise Server anterior a v8.x, póngase en contacto con Dell ProSupport para obtener asistencia).

Al actualizar/migrar Dell Enterprise Server a una nueva versión que incluya nuevas políticas introducidas 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 Dell Enterprise Server y sus componentes, seguido de la instalación/actualización del cliente.

Aplicación de cambios en la política

- 1 Inicie sesión como administrador de Dell en la Remote Management Console.
- 2 En el menú izquierdo, haga clic en **Administración > Confirmar**.
- 3 Introduzca una descripción del cambio en el campo Comentario.
- 4 Haga clic en **Confirmar políticas**.
- 5 Cuando haya finalizado la confirmación, cierre sesión en la Remote Management Console.

Asegurarse de que Dell Services se esté ejecutando

- 6 Desde 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

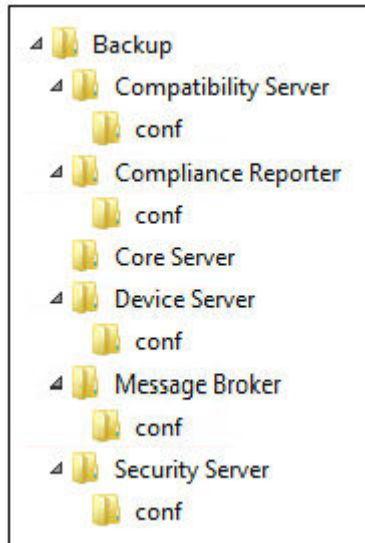
- 7 Realice una copia de seguridad de toda la instalación existente en una ubicación alternativa. La copia de seguridad debe incluir la base de datos SQL, secretKeyStore y archivos de configuración. Se necesitarán varios archivos de su instalación existente después de completar el proceso de actualización/migración.



NOTA:

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



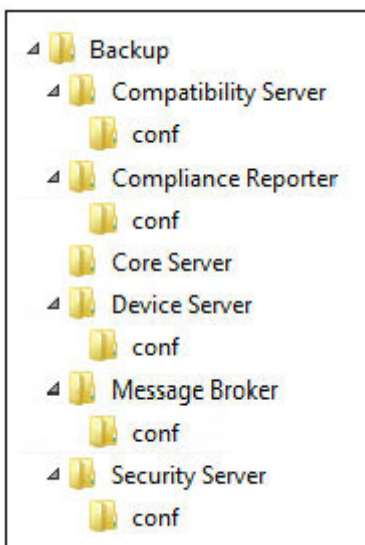


Actualización/migración de servidores back-end

- 1 En el medio de instalación de Dell, navegue hasta el directorio de Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a instalar Enterprise Server. **Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.**
- 2 Haga doble clic en **setup.exe**.
- 3 En el cuadro de diálogo *Asistente InstallShield*, seleccione el idioma para la instalación y, a continuación, 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 Autenticación de Windows, se utilizarán para la autenticación las mismas credenciales que se utilizaron para iniciar sesión en Windows (no se podrá modificar el contenido de los campos Nombre de usuario ni Contraseña).

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 Introduzca 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 el servidor.

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:

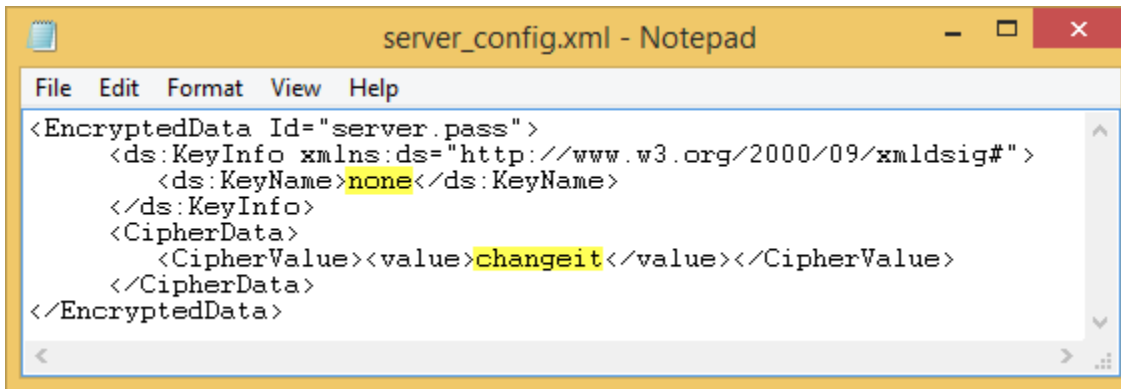
Instrucciones para server.pass:

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**.
- Introduzca la contraseña en texto legible sin formato entre las etiquetas <value> </value>, que en el ejemplo corresponde a **<value>changeit</value>**
- Cuando Dell Enterprise Server se inicie, se cifrará la contraseña en texto legible sin formato y el valor cifrado reemplazará el valor legible.

Contraseña conocida

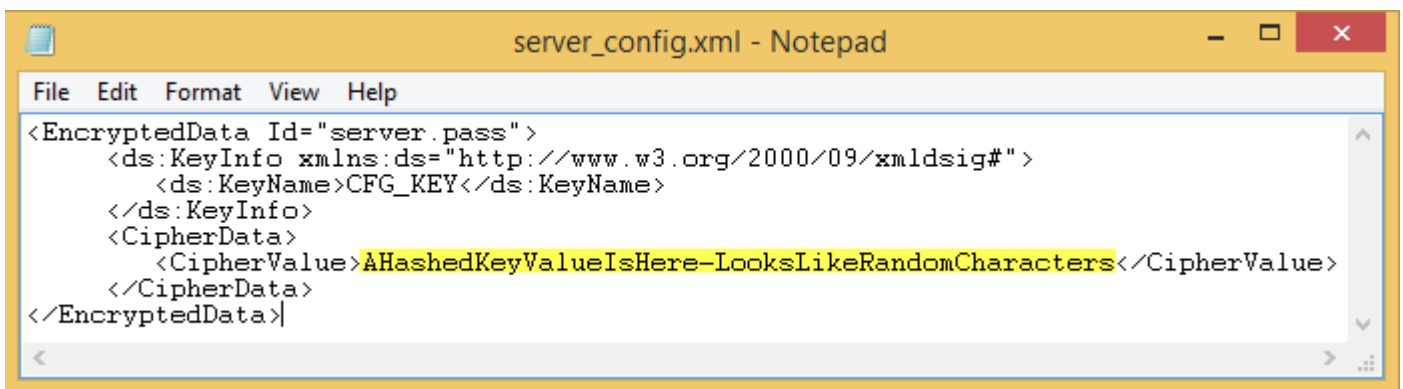




```
<EncryptedData Id="server.pass">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>none</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue><value>changeit</value></CipherValue>
  </CipherData>
</EncryptedData>
```

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



```
<EncryptedData Id="server.pass">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>CFG_KEY</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue>AHashedKeyValueIsHere-LooksLikeRandomCharacters</CipherValue>
  </CipherData>
</EncryptedData>
```

Guarde y cierre el archivo.

NOTA:

No intente cambiar la contraseña de Dell Enterprise Server 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 han completado.

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 ejecuta en modo Office protegido. Esto permite la comunicación entre cualquier dispositivo en cualquier ubicación y el servidor front-end de Dell. La política Habilitar aviso de devolución de llamada está activada de manera predeterminada. 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 Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a instalar Enterprise Server. **Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.**
- 2 Haga doble clic en **setup.exe**.
- 3 En el cuadro de diálogo *Asistente InstallShield*, seleccione el idioma para la instalación y, a continuación, 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 el servidor hasta que se completen las tareas de configuración posteriores a la instalación.

Instalación en el modo desconectado

El modo desconectado aísla Enterprise Server desde Internet, de una LAN no protegida o de otras redes no protegidas. Tras instalar Enterprise Server en modo desconectado, permanecerá en dicho modo y no se podrá volver a cambiar a modo conectado.

Enterprise Server 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 almacenarán los archivos de recuperación.

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



Parámetros

AIRGAP=1: este valor debe ser "1" para instalar Enterprise Server 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 analizará para obtener la información del servidor, instancia y puerto.

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.

IS_SQLSERVER_AUTHENTICATION=0: opcional. El valor predeterminado es 0, lo que especifica que se utilizarán las credenciales de autenticación de Windows del usuario conectado actualmente para autenticar 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 trabajan con Enterprise Server. 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 con 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 añade 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 añadir 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 guión 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.

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

SERVERPORT_CLIENTAUTH: opcional.



Parámetros

REPORTERPORT: opcional.

DEVICEPORT: opcional.

KEYSERVERPORT: opcional.

GKPORT: opcional.

TIGAPORT: opcional.

SMTP_PORT: opcional.

ACTIVEMQ_TCP: opcional.

ACTIVEMQ_STOMP: opcional.

Instalación de Enterprise Server en modo desconectado

El siguiente ejemplo instala Enterprise Server en modo silencioso con un diálogo de progreso, mediante los parámetros de instalación que se enumeran en el archivo, `C:\mysetups\eeoptions.txt` " "

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

Desinstalación de Dell Enterprise Server

- 1 En el medio de instalación de Dell, navegue hasta el directorio de Dell Enterprise Server. **Descomprima** (NO copie/pegue ni arrastre/suelte) Dell Enterprise Server-x64 en el directorio raíz del servidor en el que vaya a desinstalar Enterprise Server. ***Si copia/pega o arrastra/suelta se producirán errores y la instalación no será correcta.***
- 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**.



Configuración posterior a la instalación

Lea las *Enterprise Server Technical Advisories* (Asesorías técnicas de Enterprise Server) para ver las soluciones alternativas actuales o los problemas conocidos relacionados con la configuración de Dell Enterprise Server.

Si está instalando Dell Enterprise Server por primera vez o actualizando una instalación existente, deberá configurar algunos componentes de su entorno.

Instalación y configuración de EAS Management

Este apartado debe completarse si tiene pensado utilizar Mobile Edition. Si no es así, puede omitirla y continuar en [Configuración de Dell Security Server en modo DMZ](#).

Requisitos previos

- La cuenta de inicio de sesión para el servicio de EAS Mailbox Manager debe ser una cuenta con permisos para crear o modificar políticas de Exchange ActiveSync, asignarlas a buzones de correo de los usuarios y hacer consultas sobre los dispositivos ActiveSync.
- Para modificar archivos y reiniciar los servicios, EAS Configuration Utility se debe ejecutar con permisos de administrador.
- Se requiere conexión de red con Dell Policy Proxy.
- Tener disponible el FQDN de Dell Policy Proxy.
- Tener disponible el número de puerto de Dell Policy Proxy.
- Microsoft Message Queuing (MSMQ) ya debe estar instalado y configurado en el servidor que aloja el entorno de Exchange. Si no es así, consulte [Instalación/configuración de Microsoft Message Queuing \(MSMQ\)](#).

Pasos para realizar durante el proceso de implementación

Si va a utilizar Exchange ActiveSync para administrar dispositivos móviles con Mobile Edition, su entorno de Exchange Server debe estar configurado.

Instalar EAS Device Manager

- 1 En el medio de instalación de Dell, vaya a la carpeta EAS Management. En la carpeta EAS Device Manager, copie el archivo setup.exe en sus *Servidores de acceso de cliente de Exchange*.
- 2 Haga doble clic en **setup.exe** para iniciar la instalación. Si su entorno incluye más de un *Servidor de acceso de cliente de Exchange*, ejecute este instalador en cada uno de ellos.
- 3 Seleccione el idioma para la instalación y haga clic en **Aceptar**.
- 4 Haga clic en **Siguiente** cuando aparezca la pantalla de *Bienvenida*.
- 5 Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.
- 6 Haga clic en **Siguiente** para instalar EAS Device Manager en la ubicación predeterminada de `C:\inetpub\wwwroot\Dell\EAS Device Manager\`.
- 7 Haga clic en **Instalar** en la pantalla *Listo para comenzar la instalación*. Se mostrará una ventana de estado que muestra el progreso de la instalación.
- 8 Si lo desea, puede marcar la casilla de verificación para mostrar el registro de Windows Installer y hacer clic en **Finalizar**.



Instalar EAS Mailbox Manager

- 1 En el medio de instalación de Dell, vaya a la carpeta EAS Management. En la carpeta EAS Mailbox Manager, copie setup.exe en sus *Servidores de buzones de Exchange*.
- 2 Haga doble clic en **setup.exe** para iniciar la instalación. Si su entorno incluye más de un *Servidor de buzones de Exchange*, ejecute este instalador en cada uno de ellos.
- 3 Seleccione el idioma para la instalación y haga clic en **Aceptar**.
- 4 Haga clic en **Siguiente** cuando aparezca la pantalla de *Bienvenida*.
- 5 Lea el contrato de licencia, acepte las condiciones y haga clic en **Siguiente**.
- 6 Haga clic en **Siguiente** para instalar EAS Mailbox Manager en la ubicación predeterminada de **C:\Program Files\Dell\EAS Mailbox Manager**.
- 7 En la pantalla Información de inicio de sesión, introduzca las credenciales de la cuenta de usuario que iniciará sesión para utilizar este servicio.
Nombre de usuario: DOMINIO\Nombre de usuario

Contraseña: La contraseña asociada a este nombre de usuario

Haga clic en **Siguiente**.
- 8 Haga clic en **Instalar** en la pantalla *Listo para comenzar la instalación*.
Se mostrará una ventana de estado que muestra el progreso de la instalación.
- 9 Si lo desea, puede marcar la casilla de verificación para mostrar el registro de Windows Installer y hacer clic en **Finalizar**.

Utilizar EAS Configuration Utility

- 1 En el mismo equipo, vaya a **Inicio > Dell > EAS Configuration Utility > EAS Configuration** para ejecutar EAS Configuration Utility.
- 2 Haga clic en **Configuración** para configurar los valores de EAS Management.
- 3 Introduzca la siguiente información:
FQDN de Dell Policy Proxy

Puerto de Dell Policy Proxy (el puerto predeterminado es 8090)

Intervalo de sondeo de Dell Policy Proxy (el tiempo predeterminado es de un minuto)

Seleccione la casilla para ejecutar EAS Device Manager en modo de solo informes (recomendado durante la implementación)

NOTA:

El modo de solo informes permite a dispositivos o usuarios desconocidos acceder a Exchange ActiveSync, aunque sigue mostrando información sobre el tráfico. Una vez que la implementación esté en funcionamiento, puede cambiar esta configuración para reforzar la seguridad.

- Haga clic en **Aceptar**.
- 4 Se mostrará un mensaje de finalización satisfactoria. Haga clic en **Sí** para reiniciar los servicios de IIS y EAS Mailbox Manager Services.
 - 5 Haga clic en **Salir** cuando haya terminado.



Configuración de los valores de administración de EAS

Una vez que la implementación esté en funcionamiento, siga los pasos siguientes si desea reforzar la seguridad.

- 1 Vaya a **Inicio > Dell > EAS Configuration Utility > EAS Configuration** para ejecutar EAS Configuration Utility.
- 2 Haga clic en **Configuración** para configurar los valores de EAS Management.
- 3 Introduzca la siguiente información:
FQDN de Dell Policy Proxy

Puerto de Dell Policy Proxy (el puerto predeterminado es 8090)

Intervalo de sondeo de Dell Policy Proxy (el tiempo predeterminado es de un minuto)

Deseleccione la casilla de verificación para ejecutar EAS Device Manager en modo de solo informes

Haga clic en **Aceptar**.
- 4 Se mostrará un mensaje de finalización satisfactoria. Haga clic en **Sí** para reiniciar los servicios de IIS y EAS Mailbox Manager Services.
- 5 Haga clic en **Salir** cuando haya terminado.

Configuración de Dell Security Server en modo DMZ

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

Si se utiliza un certificado de confianza, omita esta sección y continúe con [Inscripción a APN](#).

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

Utilizar Keytool para importar el certificado de dominio DMZ

IMPORTANTE:

Realice una copia de seguridad de los cacerts de Dell Security Server existentes antes de continuar con las instrucciones de Keytool. Si se comete un error de configuración, podrá realizar el restablecimiento con el archivo guardado.

Supuestos

- Dell Security Server se ha instalado con un certificado no de confianza.
- Dell Security Server en modo DMZ se ha instalado con un certificado firmado (Entrust, Verisign, etc.)
- Se dispone de un archivo de certificado .pfx. Si el certificado debe convertirse a .pfx, consulte la sección Exportación de un certificado a .PFX mediante la consola de administración de certificados.

Proceso

- 1 Agregue Keytool a la ruta del sistema.

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

- 2 Utilice Keytool para listar el contenido del certificado de dominio de confianza que desea importar. Apunte el nombre de alias mostrado.

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



- 3 Utilice Keytool para importar el contenido del certificado firmado al archivo cacerts de Dell Security Server:

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

Para -srcalias, necesitará reunir esta información del contenido exportado del certificado firmado.

Para -destalias, puede ser cualquier ubicación de su elección.

- 4 Realice copia de seguridad del archivo cacerts actual y sustitúyalo en el directorio <directorío de instalación de Security Server>\conf\
por este archivo cacerts recién creado en Dell Security Server.

Modificar el archivo application.properties

Modifique el archivo application.properties para introducir el alias del certificado de firma.

- 1 Vaya al <directorío de instalación de Security Server>\conf\application.properties
- 2 Modifique la siguiente información:
keystore.alias.signing=<Cambie este valor por el valor del [paso 3](#) anterior para -destalias>
- 3 Reinicie el servicio de Dell Security Server.

Inscripción a APN

Si va a utilizar Mobile Edition para Seguridad de dispositivos móviles con dispositivos iOS, se debe utilizar el asistente de la inscripción a APN para:

- Crear un CSR
- Crear un certificado de inserción de Apple
- Cargar un certificado de inserción

Si no va a utilizar Mobile Edition para Seguridad de dispositivos móviles con dispositivos iOS, omita esta sección y continúe en [Herramienta de configuración del servidor](#).

El servicio de notificaciones de inserción de Apple (APN) permite la comunicación segura con dispositivos iOS a través del aire. Las APN se utilizan para enviar notificaciones de un dispositivo iOS para su comprobación con Dell Enterprise Server. Las APN solo envían notificación al dispositivo, no envían datos.

Proceso

- 1 Abra el explorador y vaya a <https://<FQDN-de-servidor-seguridad>:8443/csrweb>.
- 2 En el cuadro de diálogo Inicio de sesión del asistente de inscripción a APN, especifique sus credenciales de administrador Dell y haga clic en **Inicio de sesión**.
- 3 Aparecerá un diálogo con la descripción de los pasos que está a punto de dar. Haga clic en **Siguiente**.

Paso I: Crear CSR

- 4 Introduzca la siguiente información:

Correo electrónico: la dirección de correo electrónico puede ser cualquier UPN, pero es recomendable utilizar una cuenta para el administrador que mantenga el certificado de APN.

Nombre común: especifique el nombre común asociado con esta dirección de correo electrónico.

Haga clic en **Generar CSR**.

- 5 Después de generar un CSR, guarde el archivo en una ubicación fácilmente accesible.
- 6 Haga clic en **Siguiente**.

Paso II: Crear un certificado push de Apple



- 7 Haga clic en el vínculo del **Portal de certificados de inserción de Apple**. Inicie sesión con su Id. y contraseña de Apple.
- 8 Lea los Términos de uso, indique su aceptación y haga clic en **Aceptar**.
- 9 Haga clic en **Examinar** y, a continuación, en **Cargar** el CSR que acaba de crear.
- 10 En la página *Certificados de otros servidores*, haga clic en **Descargar**. Guarde el archivo en una ubicación fácilmente accesible.
- 11 Vuelva al asistente de inscripción a APN y haga clic en **Siguiente**.

Paso III: Subir certificado push

- 12 Introduzca la siguiente información (utilice las mismas credenciales que se utilizaron en [Paso I: Crear CSR](#)).

Correo electrónico:

Nombre común:

Archivo de certificado push: haga clic en Examinar para localizar el archivo guardado en el [paso 7](#).. Haga clic en **Cargar**.

- 13 Se mostrará un mensaje de finalización satisfactoria. Haga clic en **Finalizar**.

La inscripción del certificado APN con Dell Enterprise Server habrá finalizado.

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 de Dell Server permite:

- [Agregar certificados nuevos o actualizados](#)
- [Importar certificado Dell Manager](#)
- [Importar certificado de identidad](#)
- [Configurar los valores para el Certificado Server SSL o Mobile Edition](#)
- [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 Dell Compatibility Server no se pueden ejecutar al mismo tiempo que la Herramienta de configuración de Dell Server. Detenga el servicio de Dell Core Server y el servicio de Dell Compatibility Server en *Servicios* (**Inicio > Ejecutar**. Escriba **services.msc**) antes de iniciar la Herramienta de configuración de Dell Server.

Para iniciar la Herramienta de configuración de Dell Server, vaya a **Inicio > Programas > Dell > Enterprise Edition > Herramienta de configuración del servidor > Ejecutar Herramienta de configuración del servidor**.

La Herramienta de configuración del servidor de Dell lleva un registro de la actividad en **C:\Program Files\Dell\Enterprise Edition \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 entidad emisora pública de certificados (CA), el certificado de la CA firmante ya existirá en el almacén de certificados de Microsoft y, por lo tanto, la cadena de confianza se establecerá 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, Dell Device Server y así sucesivamente)
- Aplicaciones .NET (Dell Core Server)
- Validación de tarjetas inteligentes utilizadas para la Autenticación previa al inicio (Dell 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 de Enterprise Edition administrados remotamente con unidades de cifrado automático o BitLocker Manager.
- Estaciones de trabajo cliente:
 - Estaciones de trabajo que ejecutan BitLocker Manager
 - Estaciones de trabajo que ejecutan Enterprise Edition (clientes Windows)
 - Estaciones de trabajo que ejecutan Endpoint Security Suite
 - 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 Dell 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 keystore de Java de Dell Security Server. Para obtener más información, consulte Creación de un certificado autofirmado y generación de una solicitud de firma de certificado. Se debe importar la cadena de confianza completa.

Dell Manager:

- Introduzca 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 servidor, marque **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 utilizará la información del certificado autofirmado que se creó al instalar Enterprise Server, 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 utilizará la información del certificado autofirmado que se creó al instalar Enterprise Server, 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 utilizará la información del certificado autofirmado que se creó al instalar Enterprise Server, 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, introduzca la contraseña asociada con el certificado existente y haga clic en **Siguiente**.

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

- *Generar certificado autofirmado*: se utilizará la información del certificado autofirmado que se creó al instalar Enterprise Server, 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 Dell Enterprise Server. 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, introduzca la contraseña asociada con el certificado existente y haga clic en **Siguiente**.

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

- *Generar certificado autofirmado*: se utilizará la información del certificado autofirmado que se creó al instalar Enterprise Server, 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 de Enterprise Edition administrados remotamente con unidades de cifrado automático o BitLocker Manager, 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 Enterprise Edition administrados remotamente y a BitLocker Manager. 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 Introduzca 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 el campo *Nombre de archivo*, introduzca un nombre con el que guardar el archivo. 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 Dell Server Configuration.
- 22 En el menú superior, seleccione **Acciones > Importar certificado de Manager**.
- 23 Vaya a la ubicación donde se guardaron los archivos exportados. Seleccione el archivo y haga clic en **Abrir**.

24 Introduzca 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 de identidad

Si su implementación incluye Server Encryption, deberá importar el certificado recién creado (o existente). El certificado de identidad protege la clave privada utilizada para firmar los paquetes de políticas que se envían a servidores cliente. Este certificado puede ser independiente de cualquiera de los otros certificados.

- 1 En el menú superior, seleccione **Acciones > Importar certificado de identidad**.
- 2 Seleccione un certificado y haga clic en **Siguiente**.
- 3 En la petición de Contraseña de certificado, introduzca 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 o Mobile Edition

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, introduzca la URL del servidor que aloja SCEP.

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**.



Configuración de los valores de SMTP para Data Guardian o los servicios de correo electrónico

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

Esta pestaña configura los valores de SMTP para Data Guardian. Si la configuración de SMTP necesita configurarse por otros motivos aparte de Data Guardian, consulte el tema "Habilitación del servidor SMTP para el envío de notificaciones de licencia por correo electrónico" de la Ayuda para el administrador.

Introduzca la siguiente información:

- 1 En el campo Nombre de host:, introduzca el FQDN de su servidor SMTP, por ejemplo, nombreservidoresmtp.dominio.com.
- 2 En el campo Nombre de usuario:, introduzca el nombre de usuario con el que iniciará sesión en el servidor de correo. El formato puede ser DOMINIO\jperez, jperez, o el formato que requiera su organización.
- 3 En el campo Contraseña:, introduzca la contraseña asociada con este nombre de usuario.
- 4 En el campo Dirección de remitente:, introduzca 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 el campo Puerto:, introduzca el número de puerto (normalmente 25).
- 6 En el menú Autenticación, seleccione Verdadero o 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 el campo *Nombre de servidor*:, introduzca el nombre de dominio completo (FQDN) (si hay un nombre de 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 el campo *Puerto del servidor*:, introduzca el número de puerto.

Al utilizar una instancia de SQL Server no predeterminada, debe especificar el puerto dinámico de la instancia en el campo *Port:* (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](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx).

- 3 En el campo *Base de datos*:, introduzca el nombre de la base de datos.
- 4 En el campo *Autenticación*:, seleccione **Autenticación de Windows** o **Autenticación de SQL Server**. Si selecciona Autenticación de Windows, se utilizarán para la autenticación las mismas credenciales que se utilizaron para iniciar sesión en Windows (no se podrá modificar el contenido de los campos Nombre de usuario ni Contraseña).
- 5 En el campo *Nombre de usuario*:, introduzca el nombre de usuario adecuado asociado con esta base de datos.
- 6 En el campo *Contraseña*:, introduzca la contraseña para el nombre de usuario que aparece en el campo 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 *Prueba de configuración*, lea la información de prueba y haga clic en **Siguiente**.
- 10 Si selecciona Autenticación de Windows en la pestaña Base de datos, puede, como opción, introducir credenciales alternativas para permitir el uso de las mismas credenciales que utilizará para ejecutar Dell Enterprise Server. Haga clic en **Siguiente**.
- 11 En la ventana *Probar configuración* se mostrarán los 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](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 v8.x al esquema más reciente con la versión más reciente de la Herramienta de configuración del servidor. Para obtener la Herramienta de configuración del servidor más reciente, o para migrar una base de datos pre-v8.0, póngase en contacto con Dell ProSupport para obtener asistencia.

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

- 1 Si todavía no ha realizado copia de seguridad de su base de datos de Dell 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 hubo errores en la tarea de la base de datos y que se debe tomar 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**.



Tareas administrativas

Asignar rol de administrador Dell

- 1 Como administrador Dell, inicie sesión en Remote Management Console, en esta dirección <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 al que desee agregar un usuario.
- 4 En la página de Detalles del dominio, haga clic en la pestaña **Miembros**.
- 5 Haga clic en **Agregar usuario**.
- 6 Introduzca un filtro para buscar el Nombre de usuario por 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 un Grupo, pero no aparece en la lista de Miembros del dominio o del grupo en el Management, asegúrese de que los tres nombres para el usuario están definidos correctamente en el servidor de directorios 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 Remote Management Console Enterprise Server.
- 2 Inicie sesión en Remote Management Console Enterprise Server 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 Introduzca una descripción del cambio en el campo Comentario.
- 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*.
- 3 Se admiten dos métodos distintos de autenticación. Para configurarlos, seleccione:
 - [Configurar autenticación SQL con Compliance Reporter](#)
 - [Configurar autenticación Windows con Compliance Reporter](#)

Configurar autenticación SQL con Compliance Reporter

A partir de la versión 8.1, el origen de datos está configurado previamente listo para utilizar. No es necesaria ninguna configuración. Utilice los siguientes pasos para cambiar el origen de datos, si fuera necesario.

- 1 Para establecer el origen de datos, en el menú superior, haga clic en **Configuración**. En el menú izquierdo, haga clic en **Origen de datos**.
- 2 Escriba el nombre de usuario para iniciar sesión en la base de datos de Dell.
- 3 Escriba la contraseña para iniciar sesión en la base de datos de Dell.
- 4 Escriba el nombre de host para iniciar sesión en la base de datos de Dell.
- 5 Escriba el nombre de la base de datos para iniciar sesión en la base de datos de Dell.
- 6 Escriba la cantidad máxima de conexiones inactivas permitidas. El valor predeterminado es 2.
- 7 Escriba la cantidad máxima de conexiones (activas) permitidas. El valor predeterminado es 10.
- 8 Escriba el tiempo de espera máximo (número máximo de milisegundos que hay que esperar para una conexión). -1 es indefinidamente.
- 9 Para comprobar el URL de la base de datos y probar la conectividad entre Dell Compliance Reporter y la base de datos de Dell, haga clic en **Probar conexión**.
- 10 Haga clic en **Actualizar**. Haga clic en Cancelar para descartar la información.
Las tareas administrativas han finalizado. El resto de este capítulo trata de la autenticación de Windows y se puede omitir si se utiliza la autenticación SQL para Dell Compliance Reporter.

Si es necesario, continúe en [Creación de un certificado autofirmado y generación de una solicitud de firma de certificado](#)) o en [Exportación de un certificado a .PFX mediante la Consola de administración de certificados](#).

Configurar autenticación Windows con Compliance Reporter

A partir de la versión 8.1, el origen de datos está configurado previamente listo para utilizar. No es necesaria ninguna configuración. Utilice los siguientes pasos para cambiar el origen de datos, si fuera necesario.

- 1 Escriba el nombre de usuario para iniciar sesión en la base de datos de Dell.
- 2 Deje la contraseña en blanco. Cuando el usuario del dominio inicie sesión, su contraseña pasará a la base de datos.
- 3 Escriba el nombre de host para iniciar sesión en la base de datos de Dell.
- 4 Escriba el nombre de la base de datos para iniciar sesión en la base de datos de Dell.
- 5 Escriba la cantidad máxima de conexiones inactivas permitidas. El valor predeterminado es 2.
- 6 Escriba la cantidad máxima de conexiones (activas) permitidas. El valor predeterminado es 10.
- 7 Escriba el tiempo de espera máximo (número máximo de milisegundos que hay que esperar para una conexión). -1 es indefinidamente.



- 8 Para comprobar el URL de la base de datos y probar la conectividad entre Dell Compliance Reporter y la base de datos de Dell, haga clic en **Probar conexión**.
- 9 Haga clic en **Actualizar**. Haga clic en Cancelar para descartar la información.
Las tareas administrativas han finalizado. **Si es necesario**, continúe en [Creación de un certificado autofirmado y generación de una solicitud de firma de certificado](#)) o en [Exportación de un certificado a .PFX mediante la Consola de administración de certificados](#).

Realizar copias de seguridad

Para fines de Recuperación tras desastres, asegúrese de que se realice una copia de seguridad de las siguientes ubicaciones semanalmente, con diferenciales cada noche:

Copias de seguridad de Enterprise Server

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\gkresource.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). Como anteriormente, se recomiendan el uso de las prácticas recomendadas para la base de datos Dell y que se incluya el software Dell en el plan de recuperación tras desastres de su organización.

Para obtener información adicional sobre las mejores prácticas de SQL Server, consulte [La siguiente lista explica las prácticas recomendadas para el SQL Server, que deben implementarse cuando se instale Dell Data Protection 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.



Descripciones de los componentes Dell

La siguiente tabla describe cada componente y su función.

Nombre	Descripción	Necesario para
Compliance Reporter	Proporciona una vista amplia del entorno mediante la realización de informes de cumplimiento y auditorías. Un componente de Dell Enterprise Server.	Informes
Key Server	Negocia, autentica y cifra una conexión cliente utilizando las API de Kerberos. Requiere acceso a la base de datos SQL para extraer los datos clave. Un componente de Dell Enterprise Server.	Utilidades del administrador de Dell
Herramienta de configuración del servidor	Configura la comunicación de la base de datos con los servidores Core Server y Compatibility Server/Security Server. Se utiliza para inicializar la base de datos tras la instalación o para migrar la base de datos a un esquema más reciente. Se utiliza para controlar Dell Services. Un componente de Dell Enterprise Server.	Todo
Remote Management Console-Enterprise Server Console	Consola de administración y centro de control para implementación en toda la empresa. Un componente de Dell Enterprise Server.	Todo
Core Server	Administra el flujo de políticas, las licencias y el registro para Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat Protection. Procesa los datos de inventario para que los utilice Compliance Reporter y la Remote Management Console. Recopila y almacena datos de autenticación. Controla el acceso basado en roles. Un componente de Dell Enterprise Server.	Todo
Security Server	Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, los productos de Data Guardian, la comunicación de SED-PBA, y de Active Directory para la autenticación o la reconciliación, incluida la validación de identidades para la autenticación en la Remote Management	Todo



Nombre	Descripción	Necesario para
	Console. Requiere el acceso de base de datos SQL.	
	Un componente de Dell Enterprise Server.	
Compatibility Server	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 en función de los grupos de usuarios de este servicio.	Todo
	Un componente de Dell Enterprise Server.	
Message Broker Service	Administra la comunicación entre los servicios del Enterprise Server. Organiza la información de políticas creada por el Compatibility Server para poner en cola el policy proxy.	Todo
	Requiere el acceso de base de datos SQL.	
	Un componente de Dell Enterprise Server.	
Device Server	Permite activaciones y la recuperación de la contraseña.	Enterprise Edition para Mac
	Un componente de Dell Enterprise Server.	Enterprise Edition para Windows
		Dispositivos protectores de bolsillo
		CREDActivate
Complementos de Device Server	Ofrece compatibilidad con diversos componentes.	Todo
	Un componente de Dell Enterprise Server.	
Identity Server	Procesa las solicitudes de autenticación de dominios.	Todo
	Requiere una cuenta de Active Directory.	
	Debe ser la cuenta utilizada para acceder a SQL cuando se utiliza la autenticación de Windows.	
	Un componente de Dell Enterprise Server.	
Policy Proxy	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario.	Enterprise Edition para Mac
	Un componente de Dell Enterprise Server.	Enterprise Edition para Windows
		Mobile Edition para Seguridad de dispositivos móviles
Security Token Services (STS)	Se utiliza para ayudar a crear un canal de autenticación seguro entre la interfaz de usuario de Dell Enterprise Server y los servicios back-end de Dell.	Todo
EAS Device Manager	Habilita funciones a través del aire. Se instala en Exchange Client Access Server.	Administración Exchange ActiveSync de dispositivos móviles.

Nombre	Descripción	Necesario para
EAS Mailbox Manager	El agente del buzón que está instalado en Exchange Mailbox Server.	Administración Exchange ActiveSync de dispositivos móviles.



Prácticas recomendadas para SQL Server

La siguiente lista explica las prácticas recomendadas para el SQL Server, que deben implementarse cuando se instale Dell Data Protection 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: <http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29>
- Microsoft SQL Server 2008 R2: [http://technet.microsoft.com/en-us/library/ms190969\(v=sql.105\).aspx](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: <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29>
- 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\(v=sql.110\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.110))
- Microsoft SQL Server 2014: [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.120\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.120))
- Microsoft SQL Server 2016: [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.130\)](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: <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29>
- 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>

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

Certificados

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.

Solamente recomendamos 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, deberá 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 Dell Compliance Reporter, Dell Security Server o Dell Device Server.

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

Haga clic en **Inicio > Ejecutar** e introduzca `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 Introduzca 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 Dell Enterprise Server.

- *Contraseña de Keystore:* escriba una contraseña (los caracteres no compatibles son <> y " '), 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\eserver.properties. Establezca el valor eserver.keystore.password =

<Directorio de instalación de Security Server>\conf\eserver.properties. Establezca el valor eserver.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 completo incluye el nombre de host y el nombre de dominio (ejemplo, server.domain.com).
- *Unidad organizacional:* introduzca el valor adecuado (ejemplo: Seguridad).
- *Organización:* introduzca el valor correspondiente (ejemplo: Dell).
- *Ciudad o localidad:* introduzca el valor adecuado (ejemplo: Dallas).
- *Estado o provincia:* introduzca 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 introducido 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 introduce 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](#).

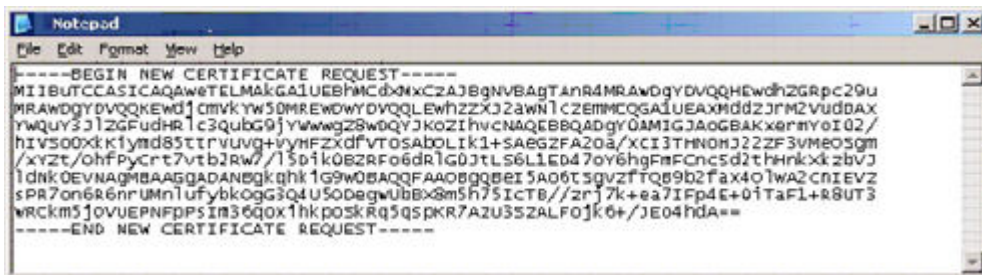
- 1 Sustituya el mismo valor utilizado anteriormente para **<certificatalias>**:

```
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 contendrá un par BEGIN/END que se utilizará 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. Esta copia de seguridad evitará 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 Dell Compliance Reporter, Dell Security Server o Dell Device Server, cambie al directorio **conf** del componente.
 - Si habilita SSL entre Dell Enterprise Server y el servidor de directorio Enterprise, 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 explorador web para 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 proporcionará 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. Vuelva a la ventana de DOS. 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 Al mostrar el archivo cacerts se verá 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 file en MMC, deberá convertirlo en un archivo .pfx para su uso con Keytool cuando Dell Security Server se utilice en el modo DMZ y al importar un certificado de Dell Manager a la Herramienta de configuración de Dell Server.

- 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 Introduzca 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 el campo *Nombre de archivo*, introduzca un nombre con el que guardar el archivo. 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.

