

DDP Enterprise Server - Virtual Edition

Guía de inicio rápido y Guía de instalación 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, 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 registradas de Google Inc. en Estados Unidos y 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 registradas de Apple, Inc. en Estados Unidos y otros países. GO ID®, RSA® y SecurID® son marcas comerciales registradas de Dell EMC. EnCase™ y Guidance Software® son marcas comerciales o marcas 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). Virtual Edition utiliza bibliotecas de terceros de "urwid" bajo los términos de la Licencia pública general reducida de GNU. El aviso de copyright y la Licencia pública general reducida de GNU se pueden encontrar en AdminHelp en la página Asignaciones, copyrights y marcas comerciales.

Guía de inicio rápido y Guía de instalación de VE

2017 - 04

Rev. A01

Tabla de contenido

| | |
|---|-----------|
| 1 Guía de instalación y de inicio rápido de Virtual Edition..... | 5 |
| Instalación de DDP Enterprise Server - VE..... | 5 |
| Configuración de VE..... | 5 |
| Abrir la Remote Management Console VE..... | 5 |
| Tareas administrativas..... | 6 |
| 2 Guía de instalación de Virtual Edition..... | 7 |
| Acerca de DDP Enterprise Server - VE..... | 7 |
| Cómo ponerse en contacto con Dell ProSupport..... | 7 |
| Requisitos..... | 7 |
| Requisitos previos de DDP Enterprise Server - VE..... | 7 |
| Requisitos previos de la Remote Management Console VE..... | 9 |
| Requisitos previos del modo de proxy..... | 9 |
| Descargar DDP Enterprise Server - VE..... | 10 |
| Instalación de DDP Enterprise Server - VE..... | 11 |
| Abrir la Remote Management Console VE..... | 12 |
| Instalación y configuración del modo de proxy..... | 12 |
| Terminal de VE - Tareas de configuración básicas..... | 14 |
| Cambiar el nombre de host..... | 14 |
| Cambiar la configuración de red..... | 14 |
| Establecer el nombre de host de DMZ..... | 14 |
| Cambiar la zona horaria..... | 15 |
| Actualización de DDP Enterprise Server - VE..... | 15 |
| Cambiar contraseñas de usuario..... | 16 |
| Configurar usuarios de Transferencia de archivos (FTP)..... | 17 |
| Habilitar SSH..... | 17 |
| Iniciar detener servicios de VE..... | 17 |
| Reiniciar VE..... | 18 |
| Cerrar VE..... | 18 |
| Terminal de VE - Tareas de configuración avanzadas..... | 18 |
| Establecer o cambiar la contraseña de la base de datos..... | 18 |
| Configurar valores de SMTP..... | 18 |
| Importar un certificado existente o registrar un certificado de servidor nuevo..... | 19 |
| Configurar la rotación de registros..... | 20 |
| Realizar copias de seguridad y restaurar..... | 20 |
| Habilitar el acceso remoto a la base de datos..... | 22 |
| Habilitar la compatibilidad del servidor DMZ..... | 22 |
| 3 DDP Enterprise Server - Tareas del administrador VE..... | 23 |
| Establecer o cambiar el idioma de terminal de DDP Enterprise Server - VE..... | 23 |
| Comprobar el estado del servidor..... | 23 |
| Ver registros..... | 24 |
| Abrir la interfaz de la línea de comandos..... | 24 |



| | |
|---|-----------|
| Generar un registro de instantáneas del sistema..... | 24 |
| 4 Mantenimiento de DDP Enterprise Server - VE..... | 26 |
| 5 Solución de problemas de DDP Enterprise Server - VE..... | 27 |
| 6 Tareas de configuración posteriores a la instalación..... | 28 |
| Configurar VE para Data Guardian..... | 28 |
| Instalar y configurar EAS Management para Mobile Edition..... | 28 |
| Habilitar comprobación de cadenas de confianza del administrador..... | 30 |
| 7 Tareas del administrador de la Remote Management Console VE..... | 31 |
| Asignar rol de administrador Dell..... | 31 |
| Iniciar sesión con rol de administrador Dell..... | 31 |
| Confirmar políticas..... | 32 |
| 8 Puertos de la solución..... | 33 |



Guía de instalación y de inicio rápido de Virtual Edition

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

Si desea obtener instrucciones más detalladas, consulte la [Guía de instalación de Virtual Edition](#).

Para obtener más información sobre los requisitos previos de VE, consulte [Requisitos previos de DP Enterprise Server - VE](#), [Requisitos previos de Remote Management Console](#) y [Requisitos previos del modo de proxy](#).

Para obtener información sobre cómo actualizar DDP Enterprise Server - VE, consulte [Actualización de DDP Enterprise Server - VE](#).

Instalación de DDP Enterprise Server - VE

- 1 Vaya al directorio en el que están almacenados los archivos de Dell Data Protection y haga doble clic para importarlos a VMWare **DDP Enterprise Server - VE v9.x.x Build x.ova**.
- 2 Encienda DDP Enterprise Server - VE.
- 3 Siga las instrucciones que se muestran en pantalla.

Configuración de VE

Antes de activar usuarios, debe completar las siguientes tareas de configuración en la terminal de DDP Enterprise Server - VE:

- [Establecer o cambiar la contraseña de la base de datos](#)
- [Configurar valores de SMTP](#)
- [Importar un certificado existente o registrar un certificado de servidor nuevo](#)
- [Actualización de DDP Enterprise Server - VE](#)
- Instalación de un cliente FTP compatible con SFTP en el puerto 22 y [Configuración de usuarios de Transferencia de archivos \(FTP\)](#).

Si su organización cuenta con dispositivos externos, consulte [Instalar y configurar el modo de proxy](#).

i **NOTA:** Si sus clientes Enterprise Edition estarán autorizados por la 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 mismo servidor que ejecuta Virtual 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.

Abrir la Remote Management Console VE

Abra la Remote Management Console VE en esta dirección:

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

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



Para obtener una lista de los exploradores web admitidos, consulte los [Requisitos previos de Remote Management Console VE](#).

Tareas administrativas

Si aún no ha iniciado la Remote Management Console VE, hágalo ahora. Las credenciales predeterminadas son **superadmin/changeit**.

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

Haga clic en “?” en la esquina superior derecha de la Remote Management Console VE para iniciar la *Ayuda del administrador de Dell Data Protection*. Aparecerá la página *Introducción*. Haga clic en **Agregar dominios**.

A modo de línea base, hay políticas que están establecidas para su organización, pero es posible que necesiten ser modificadas según sus requisitos específicos, de la forma siguiente (la concesión de licencias y autorizaciones rige todas las activaciones):

- Se cifran los equipos Windows
- Se cifran los equipos que tienen unidades de cifrado automático
- No se habilita la administración de BitLocker
- No se habilita Advanced Threat Protection
- Se ha habilitado Threat Protection
- No se cifran los soportes externos
- No se cifran los dispositivos conectados a puertos
- Dell Data Guardian está activado
- No se habilita Mobile Edition

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

Las tareas de la guía de inicio rápido han finalizado.



Guía de instalación de Virtual Edition

Esta Guía de instalación está dirigida a usuarios con menos experiencia, para instalar y configurar DDP Enterprise Server - VE. Como regla general, Dell recomienda instalar primero DDP Enterprise Server - VE y, a continuación, realizar la instalación de los clientes.

Para obtener información sobre cómo actualizar DDP Enterprise Server - VE, consulte [Actualización de DDP Enterprise Server - VE](#).

Acerca de DDP Enterprise Server - VE

DDP Enterprise Server - VE es la parte de administración de la seguridad de la solución de Dell. La Remote Management Console VE permite que los administradores controlen el estado de los extremos, el cumplimiento de políticas y la protección en toda la empresa. Proxy Mode ofrece una opción del modo DMZ front-end que se puede utilizar con DDP Enterprise Server - VE.

DDP Enterprise Server - VE tiene las siguientes características:

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

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell 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

Requisitos previos de DDP Enterprise Server - VE

Hardware

El espacio en disco recomendado para DDP Enterprise Server - VE es de 80 GB.



Entorno virtualizado

DDP Enterprise Server - VE v9.6 se ha validado con los siguientes entornos virtualizados.

Entornos virtualizados

- VMware Workstation 12.5
 - CPU de 64 bits, necesario
 - 4 GB de RAM, recomendado
 - Consulte <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> para obtener una lista completa de los sistemas operativos host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Consulte <http://pubs.vmware.com/workstation-11/index.jsp> para obtener más información
- VMWare Workstation 11
 - CPU de 64 bits, necesario
 - 4 GB de RAM, recomendado
 - Consulte <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> para obtener una lista completa de los sistemas operativos host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Consulte <http://pubs.vmware.com/workstation-11/index.jsp> para obtener más información
- VMWare ESXi 6.0
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo
 - Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Consulte <http://pubs.vmware.com/vsphere-60/index.jsp> para obtener más información.
- VMWare ESXi 5.5
 - CPU de 64 bits x86, necesario
 - Equipo host con un mínimo de dos núcleos
 - 8 GB de RAM como mínimo, recomendado
 - No es necesario un sistema operativo
 - Consulte <http://www.vmware.com/resources/compatibility/search.php> para obtener una lista completa de sistemas operativos de host admitidos
 - El hardware debe cumplir con los requisitos mínimos de VMWare
 - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
 - Para obtener más información, consulte <http://pubs.vmware.com/vsphere-55/index.jsp>.
- 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



Entornos virtualizados

- 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>.

Requisitos previos de la Remote Management Console VE

Navegadores de Internet

NOTA:

Su navegador debe aceptar cookies.

La siguiente tabla muestra los navegadores de Internet admitidos.

Navegadores de Internet

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

Requisitos previos del modo de proxy

Hardware

La tabla siguiente muestra los requisitos *mínimos* de hardware del modo de proxy.

Procesador

2 GHz Core 2 Duo o superior

RAM

+2 GB de RAM dedicada como mínimo/se recomiendan 4 GB de memoria RAM dedicada

Espacio libre en disco

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

Tarjeta de red

Tarjeta de interfaz de red de 10/100/1000

Varios

Protocolo TCP/IP instalado y activado

Software

La tabla a continuación indica el software que debe estar presente antes de instalar el modo de proxy.



Requisitos previos

- **Windows Installer 4.0 o posterior**

Windows Installer 4.0 o posterior debe estar instalado en el servidor en el que se vaya a hacer la instalación.

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

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

- **Microsoft .NET Framework versión 4.5**

Microsoft ha publicado actualizaciones de seguridad para .NET Framework versión 4.5

La tabla a continuación indica los requisitos de software para el servidor del modo de proxy.

① **NOTA:**

Siempre deshabilite UAC al utilizar Windows Server 2008. Una vez que UAC esté deshabilitado, el servidor debe reiniciarse para que el cambio tenga efecto.

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

Sistema operativo

- **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

Descargar DDP Enterprise Server - VE

En la instalación inicial, DDP Enterprise Server - VE se entrega como un archivo OVA, una Aplicación virtual abierta utilizada para entregar software que se ejecuta en una máquina virtual. El archivo OVA de DDP Enterprise Server - VE está disponible en www.dell.com/support, en las páginas de Asistencia del producto para los siguientes productos de Dell Data Protection:

Cifrado

O bien



Endpoint Security Suite

O bien

Endpoint Security Suite Enterprise

O bien

Data Guardian

Para descargar el archivo OVA:

- 1 Vaya a la página de asistencia del producto para [cifrado](#), [Endpoint Security Suite](#), [Endpoint Security Suite Enterprise](#) o [Data Guardian](#).
- 2 Haga clic en **Controladores y descargas**.
- 3 Junto a "Ver todas las actualizaciones disponibles para <versión del sistema operativo> ", haga clic en **Cambiar SO**, y seleccione una de las siguientes opciones: **VMware ESXi 6.0**, **VMware ESXi 5.5**, o **VMware ESXi 5.1**.
- 4 Bajo "Ver por:" seleccione **Mostrar todo**.
- 5 Bajo Dell Data Protection, seleccione **Descargar**.

Instalación de DDP Enterprise Server - VE

Antes de comenzar, asegúrese de que se cumplan todos los [Requisitos](#) de los entornos virtualizados y del sistema.

- 1 Localice los archivos Dell Data Protection en el soporte de instalación y haga doble clic para importarlos a VMWare **DDP Enterprise Server - VE v9.x.x Build x.ova**.
- 2 Encienda DDP Enterprise Server - VE.
- 3 Seleccione el idioma para el contrato de licencia y, a continuación, seleccione **Mostrar CLUF**.
- 4 Lea el contrato y seleccione **Aceptar CLUF**.
- 5 Si hay una actualización disponible, seleccione **Aceptar**.
- 6 Seleccione **Modo predeterminado** o **Modo desconectado**.



NOTA:

Si selecciona **Modo desconectado**, VE nunca puede cambiarse al modo predeterminado.

El modo desconectado aísla VE desde Internet, de una LAN no protegida o de otras redes no protegidas. Todas las actualizaciones deben realizarse manualmente. Para obtener más información sobre la funcionalidad de modo desconectado y sus políticas, consulte *AdminHelp* (Ayuda del administrador).

- 7 En la solicitud de cambio de contraseña predeterminada, seleccione **Sí**.
- 8 En la pantalla *Establecer contraseña ddpuser*, introduzca la contraseña actual (predeterminada), **ddpuser**; a continuación, introduzca una contraseña exclusiva, vuelva a introducir la contraseña exclusiva y seleccione **Aceptar**.

Las contraseñas deben incluir lo siguiente:

- Al menos ocho caracteres
 - Al menos una letra mayúscula
 - Al menos un dígito
 - Al menos 1 carácter especial
- 9 En el diálogo *Configurar nombre de host*, use la tecla de retroceso para borrar el nombre de host predeterminado. Introduzca un nombre de host exclusivo y seleccione **Aceptar**.
 - 10 En el cuadro de diálogo *Configurar valores de red*, elija una de las opciones siguientes y seleccione **Aceptar**.
 - (Predeterminado) Usar DHCP.
 - (Recomendado) en el campo Usar DHCP, pulse la barra espaciadora para extraer la X e introduzca manualmente estas direcciones, según corresponda: Puerta de enlace predeterminada de la máscara de red IP estática Servidor DNS 1 Servidor DNS 2 Servidor DNS 3



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

- 11 En la pantalla *Zona horaria*, utilice las flechas del teclado para resaltar su zona horaria y seleccione **Intro**.
- 12 En la solicitud de confirmación de zona horaria, seleccione **Aceptar**.
- 13 Cuando se muestre el mensaje que indica que la configuración inicial ha finalizado, seleccione **Aceptar**.
- 14 [Establecer o cambiar la contraseña de la base de datos](#).
- 15 [Configurar valores de SMTP](#).
- 16 [Importar un certificado existente o registrar un certificado de servidor nuevo](#).
- 17 [Actualización de DDP Enterprise Server - VE](#).
- 18 Instalación de un cliente FTP compatible con SFTP en el puerto 22 y [Configuración de usuarios de Transferencia de archivos \(FTP\)](#).

Se han completado las tareas de instalación de DDP Enterprise Server - VE.

Abrir la Remote Management Console VE

Abra la Remote Management Console VE en esta dirección:

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

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

Para obtener una lista de los exploradores web admitidos, consulte los [Requisitos previos de Remote Management Console VE](#).

Instalación y configuración del modo de proxy

El modo de proxy ofrece una opción de front-end (modo DMZ) para su uso con DDP Enterprise Server - VE. 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 VE. **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.

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**.

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

Terminal de VE - Tareas de configuración básicas

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

Cambiar el nombre de host

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

- 1 En el menú *Configuración básica*, seleccione **Nombre de host**.
- 2 Use la tecla de retroceso para borrar el nombre de host de DDP Enterprise Server - VE existente y, a continuación, introduzca el nuevo nombre de host y seleccione **Aceptar**.

Cambiar la configuración de red

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

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

IP estática

Máscara de red

Puerta de enlace predeterminada

Servidor DNS 1

Servidor DNS 2

Servidor DNS 3

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

Establecer el nombre de host de DMZ

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

- 1 En el menú *Configuración básica*, seleccione **Nombre de host de DMZ**.
- 2 Introduzca el nombre de dominio completo del servidor DMZ y seleccione **Aceptar**.

 **NOTA:** Para utilizar Modo Proxy (modo DMZ), debe instalar y configurar el modo Proxy.

Cambiar la zona horaria

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

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

Actualización de DDP Enterprise Server - VE

Para obtener más información sobre una actualización específica, consulte las consultas técnicas de VE, que se encuentra en el sitio web del servicio de asistencia de Dell en <http://www.dell.com/support>. Para ver la versión y la fecha de instalación de una actualización que ya está aplicada, en el menú **Configuración básica**, seleccione **Actualizar DDP Enterprise Server - VE > Última actualización correcta aplicada**.

Para recibir notificaciones de correo electrónico cuando estén disponibles las actualizaciones de VE, consulte [Configurar valores de SMTP](#).

NOTA: En el modo predeterminado, debe actualizarse tras la instalación inicial de DDP Enterprise Server - VE y también antes de activar los clientes.

Si los cambios de política se han realizado pero no se han confirmado en la Remote Management Console, aplique los cambios de política antes de actualizar VE:

- 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.

Actualización de VE (modo predeterminado)

- 1 Dell recomienda realizar una copia de seguridad periódicamente. Antes de actualizar, asegúrese de que el proceso de copia de seguridad ha estado funcionando correctamente. Consulte [Realizar copias de seguridad y restaurar](#).
- 2 Del menú **Configuración básica**, seleccione **Actualizar DDP Enterprise Server - VE**.
- 3 Seleccione la acción deseada:
 - Establecer el servidor de actualización: seleccione esta opción para establecer o cambiar la ubicación del servidor en la que se guardan los paquetes de actualización de DDP Enterprise Server - VE. En la pantalla *Establecer servidor de actualizaciones*, use la tecla de retroceso para borrar la dirección IP o el nombre de host del servidor actuales. Introduzca la nueva dirección IP o el nuevo nombre de dominio completo y seleccione **Aceptar**.

El servidor de actualización predeterminado es **act.credant.com**.

- Establecer la configuración Proxy: seleccione esta opción para establecer la configuración Proxy para descargar actualizaciones.

En la pantalla **Configurar valores Proxy**, presione la barra espaciadora para introducir una **X** en el campo Utilizar Proxy. Introducir las direcciones Proxy FTP, HTTP, HTTPS. Si es necesaria una autenticación de firewall, presione la barra espaciadora para introducir una **X** en el campo Autenticación necesaria. Introduzca el nombre de usuario y contraseña y presione **Aceptar**.

NOTA: Para hacer la actualización desde un sitio FTP, escriba el nombre de usuario y la contraseña de FTP e indique la URL.

- Buscar actualizaciones: seleccione esta opción para comprobar si hay un paquete de actualización de DDP Enterprise Server - VE en el servidor de actualizaciones.



- Descargar actualizaciones: seleccione esta opción para descargar una actualización después de que la detecte la función Buscar actualizaciones.
- Aplicar actualizaciones: seleccione esta opción si desea aplicar un paquete de actualización de DDP Enterprise Server - VE que haya descargado. En la pantalla *Seleccionar un archivo de actualización (.deb)*, seleccione el paquete de actualización que desea instalar y presione **Intro**.
- Última actualización correcta aplicada: seleccione esta opción para ver la versión y la fecha de instalación de la versión de VE actual.

Actualización de VE (modo desconectado)

- 1 Dell recomienda realizar una copia de seguridad periódicamente. Antes de actualizar, asegúrese de que el proceso de copia de seguridad ha estado funcionando correctamente. Consulte [Realizar copias de seguridad y restaurar](#).
- 2 Obtenga el archivo .deb que contiene la última actualización de VE en el sitio web de asistencia de Dell.
Las descargas de VE se encuentran en la carpeta **Controladores y descargas** en

www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

O bien

www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

O bien

www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

O bien

www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

- 3 Almacene el archivo .deb en la carpeta /updates en el servidor FTP seguro de VE.
Asegúrese de que el cliente de FTP admite SFTP en el puerto 22 y que el usuario de FTP está configurado. Consulte [Configurar usuarios de Transferencia de archivos \(FTP\)](#).
- 4 Del menú **Configuración básica**, seleccione **Actualizar DDP Enterprise Server - VE**.
- 5 Seleccione **Aplicar actualización** y pulse **Intro**.
Si el archivo .deb no se muestra, asegúrese de que [el archivo .deb está almacenada en la ubicación adecuada](#).
- 6 Seleccione el archivo de actualización .deb que desea instalar y pulse **Intro**.

Cambiar contraseñas de usuario

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

Puede cambiar las contraseñas de los usuarios siguientes:

- ddpuser (Administrador de terminal de DDP Enterprise Server): este usuario tiene acceso al Terminal VE y a sus menús.
 - ddpconsole (Acceso a Shell de DDP Enterprise Server - VE): este usuario tiene acceso a shell VE. El acceso a Shell está disponible para que el administrador de red compruebe y lleve a cabo soluciones de problemas en la red.
 - ddpsupport (Administrador de Dell ProSupport): este usuario existe solo para el uso de Dell ProSupport. Por motivos de seguridad, es usted el que controla la contraseña de esta cuenta.
- 1 En el menú *Configuración básica*, seleccione **Cambiar contraseñas de usuario**.
 - 2 En la pantalla *Cambiar contraseñas de usuario*, seleccione la contraseña de usuario que desee cambiar y presione **Intro**.
 - 3 En la pantalla *Establecer contraseña*, introduzca la contraseña actual y la contraseña nueva, vuelva a introducir la contraseña nueva y seleccione **Aceptar**.

Las contraseñas deben incluir lo siguiente:

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

Configurar usuarios de Transferencia de archivos (FTP)

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

Puede dar acceso al servidor FTP seguro de DDP Enterprise Server - VE a un máximo de tres usuarios para las tareas de copia de seguridad y restauración. El servidor FTP de VE también se puede utilizar para almacenar o cargar actualizaciones en DDP Enterprise Server - VE.

- 1 En el menú *Configuración básica*, seleccione **Usuarios de Transferencia de archivos (FTP)**.
- 2 En la pantalla **Configurar usuarios de FTP**, para habilitar un usuario de FTP, presione la barra espaciadora para introducir una **X** en el campo Estado del usuario. Para deshabilitar un usuario de FTP, presione la barra espaciadora para borrar la **X** del campo Estado del usuario.
- 3 Introduzca un nombre de usuario y contraseña para el usuario de SFTP.
Las contraseñas deben incluir lo siguiente:
 - Al menos ocho caracteres
 - Al menos una letra mayúscula
 - Al menos un dígito
 - Al menos 1 carácter especial
- 4 Cuando haya terminado de agregar usuarios de SFTP, seleccione **Aceptar**.

Habilitar SSH

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

Puede habilitar SSH para el inicio de sesión de Administrador de soporte, el acceso al shell de DDP Enterprise Server - VE y la interfaz de línea de comandos de terminal de VE.

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

Iniciar detener servicios de VE

Realice esta tarea solo si es necesario. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

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

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



Reiniciar VE

Realice esta tarea solo si es necesario.

- 1 En el menú *Configuración básica*, seleccione **Reiniciar appliance**.
- 2 En la solicitud de confirmación, seleccione **Sí**.
- 3 Después de reiniciar, inicie sesión en DDP Enterprise Server - VE.

Cerrar VE

Realice esta tarea solo si es necesario.

- 1 En el menú *Configuración básica*, desplácese hasta abajo y seleccione **Apagar appliance**.
- 2 En la solicitud de confirmación, seleccione **Sí**.
- 3 Después de reiniciar, inicie sesión en DDP Enterprise Server - VE.

Terminal de VE - Tareas de configuración avanzadas

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

Establecer o cambiar la contraseña de la base de datos

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.


- 1 En el menú *Configuración avanzada*, seleccione **Contraseña de la base de datos**.
- 2 Introduzca una contraseña para acceder a la base de datos y seleccione **Aceptar**.

Las contraseñas deben incluir lo siguiente:

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

 **NOTA:** Dell le recomienda hacer copias de seguridad de las contraseñas al terminar el proceso de instalación.

Configurar valores de SMTP

Para recibir notificaciones de correo electrónico de DDP Enterprise Server - VE  para utilizar Data Guardian, siga los pasos de esta sección para establecer la configuración de SMTP. Las notificaciones de correo electrónico de DDP Enterprise Server - VE informan a los destinatarios sobre estados de error del servidor de DDP Enterprise Server - VE, actualizaciones de contraseña, disponibilidad de actualizaciones de DDP Enterprise Server - VE y problemas de licencias de cliente.

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

Para establecer la configuración de SMTP, siga estos pasos:

- 1 En el menú *Configuración avanzada*, seleccione **Notificaciones de correo electrónico**.
- 2 En la pantalla *Configurar notificaciones de correo electrónico*, para habilitar las alertas de correo electrónico, presione la barra espaciadora para introducir una **X** en el campo *Habilitar alertas de correo electrónico*.

- 3 Introduzca el nombre de dominio completo del servidor SMTP.
- 4 Introduzca el puerto SMTP.
- 5 En el campo Del usuario, introduzca la Id. de la cuenta de correo electrónico que enviará las notificaciones.
- 6 En el campo Introducir usuario, introduzca la Id. de la cuenta de correo electrónico de acceso para cambiar las notificaciones configuradas.
- 7 En el campo Contraseña, introduzca una contraseña de acceso para cambiar las notificaciones de correo electrónico configuradas.
- 8 En los campos de los Id. de correo electrónico para Estado de VE, Actualizaciones de contraseña y Disponibilidad de actualizaciones, escriba las listas de destinatarios para cada tipo de notificación. Siga las siguientes convenciones al crear las listas de destinatarios:
 - El formato de dirección de correo electrónico es destinatario@dell.com.
 - Los destinatarios se deben separar con coma o punto y coma.
- 9 En el campo Recordatorio de alerta de servicio, para habilitar los recordatorios, presione la barra espaciadora para introducir una **X** en el campo y, a continuación, establezca el intervalo del recordatorio en minutos. Se desencadena un Recordatorio de alerta de servicio cuando se pasa el intervalo del recordatorio después de que una notificación se haya enviado sobre un problema de estado del sistema y el host o los servicios permanezcan en el mismo estado.
- 10 En el campo Informe de resumen, para habilitar los informes de notificaciones, seleccione el intervalo deseado (Diariamente, semanalmente o mensualmente) y, a continuación, presione la barra espaciadora para introducir una **X** en el campo.
- 11 Seleccione **Aceptar**.

Importar un certificado existente o registrar un certificado de servidor nuevo

Para poder activar los usuarios de DDP Enterprise Server - VE, los certificados deben estar disponibles.

Por medio de DDP Enterprise Server - VE, puede importar un certificado existente o crear una solicitud de certificado.

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

Importar un certificado existente de servidor

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

 **NOTA:** Conserve la contraseña de exportación porque la necesitará cuando importe el certificado en DDP Enterprise Server - VE.

- 2 En el servidor FTP de DDP Enterprise Server - VE, almacene el certificado en **/opt/dell/vsftpd/files/certificates**.
- 3 En el menú *Configuración avanzada* de DDP Enterprise Server - VE, seleccione **Certificados de servidor**.
- 4 Seleccione **Importar certificado existente**.
- 5 Seleccione un archivo de certificado para instalar en DDP Enterprise Server - VE.
- 6 Cuando se le solicite, introduzca la contraseña de exportación del certificado y seleccione **Aceptar**.
- 7 Cuando se complete el proceso de importación, seleccione **Aceptar**.

Suscribir un nuevo certificado de servidor

- 1 En el menú *Configuración avanzada*, seleccione **Certificados de servidor**.
- 2 Seleccione **Certificado de servidor nuevo**.
- 3 Seleccione **Crear solicitud de certificado**.
- 4 Complete los campos de la pantalla *Generar solicitud de certificado*:
 - Código del país: código de dos letras del país.
 - Estado/provincia: introduzca el nombre de la provincia o el estado sin abreviar (por ejemplo, Texas).
 - *Nombre de la localidad/ciudad*: introduzca el valor adecuado (por ejemplo, Dallas).
 - Organización: introduzca el valor correspondiente (por ejemplo, Dell).



- *Unidad organizacional*: introduzca el valor adecuado (por ejemplo, Seguridad).
 - *Nombre común*: introduzca el nombre de dominio completo del servidor en el que esté instalado DDP Enterprise Server - VE. Este nombre de dominio completo incluye el nombre de host y el nombre de dominio (por ejemplo: servidor.dominio.com).
 - *Id. de correo electrónico*: introduzca la dirección de correo electrónico a la que se deberá enviar su CSR.
- 5 Siga el proceso de su organización para la adquisición de un certificado de servidor SSL de una autoridad de certificación. Envíe el contenido del archivo CSR para su firma.
 - 6 Cuando reciba el certificado firmado, expórtelo como archivo .p7b y descargue la cadena de confianza completa en formato .der.
 - 7 Haga copias de seguridad del certificado y la cadena de confianza.
 - 8 Cargue el archivo del certificado y su cadena de confianza entera al servidor FTP de DDP Enterprise Server - VE.
 - 9 En el menú *Configuración avanzada*, seleccione **Certificados de servidor**.
 - 10 Seleccione **Certificado de servidor nuevo**.
 - 11 Seleccione *Certificado de suscripción completado*.
 - 12 Seleccione el archivo de certificado para instalar en DDP Enterprise Server - VE.
 - 13 Si se le solicita, especifique la contraseña del certificado: **changeit**.

Para habilitar la validación de confianza en clientes de Encryption basados en Windows, consulte Enable Manager Trust Chain Check (Habilitar comprobación de cadenas de confianza del administrador).

Crear e instalar un certificado autofirmado

- 1 En el menú *Configuración avanzada* de DDP Enterprise Server - VE, seleccione **Certificados de servidor**.
- 2 Seleccione **Crear e instalar certificados autofirmados**.
- 3 Para confirmar que desea reemplazar un certificado instalado previamente con un nuevo certificado, haga clic en **Si**.
- 4 Introduzca la contraseña del certificado: **changeit**.
- 5 Una vez que se haya instalado el nuevo certificado, seleccione **Aceptar** y espere a que se reinicien los servicios.

Los servicios VE se reinician automáticamente.

Configurar la rotación de registros

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

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

Para deshabilitar la rotación de registros, use la barra espaciadora para introducir una **X** en el campo Sin rotación y seleccione **Aceptar**.

Para habilitar la rotación de registros, siga estos pasos:

- 1 Para habilitar una rotación diaria, semanal o mensual, use la barra espaciadora para introducir una **X** en el campo correspondiente. Para rotaciones semanales o mensuales, indique el día de la semana o el mes como numeral, donde Lunes=1.
- 2 Introduzca la hora de la rotación en el campo "Hora de rotación de registros".
- 3 Seleccione **Aceptar**.

Realizar copias de seguridad y restaurar

Las copias de seguridad se pueden configurar o realizar en cualquier momento y no son necesarias para empezar a utilizar DDP Enterprise Server - VE. Dell recomienda configurar un proceso de copia de seguridad periódico.

Las copias de seguridad se pueden almacenar en un servidor FTP seguro externo (recomendado) o en DDP Enterprise Server - VE. Si se almacenan en el VE Server cuando el disco esté al 90 por ciento de su capacidad, no se almacenarán las copias de seguridad más nuevas. Recibirá una notificación de correo electrónico en la que se indicará que el espacio de asignación del disco está en un nivel bajo.

NOTA:

Para conservar el espacio de partición en disco y evitar la eliminación automática de las copias de seguridad, elimine copias de seguridad innecesarias de DDP Enterprise Server - VE.

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

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

- 1 Para habilitar las copias de seguridad diarias, semanales o mensuales, use la barra espaciadora para introducir una **X** en el campo correspondiente. Para copias de seguridad semanales o mensuales, indique el día de la semana o el mes como numeral, donde Lunes=1. Para deshabilitar las copias de seguridad, use la barra espaciadora para introducir una **X** en el campo Sin copia de seguridad y seleccione **Aceptar**.
- 2 Introduzca la hora de la copia de seguridad en el campo "Hora de copia de seguridad".
- 3 Seleccione **Aceptar**.

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

NOTA:

Antes de comenzar una operación de Restauración, deben estar en ejecución todos los servicios del VE Server. [Comprobar estado del servidor](#). Si no están en ejecución todos los servicios, reinícelos. Para obtener más información, consulte [Iniciar o detener servicios de VE](#). Empiece a restaurar **solo** cuando **todos** los servicios estén en ejecución.

Para hacer una restauración a partir de una copia de seguridad, en el menú *Configuración avanzada*, seleccione **Copia de seguridad y restauración > Restaurar** y seleccione el archivo de copia de seguridad que desee restaurar. En la pantalla de confirmación, seleccione **Sí**.

VE se reinicia y la copia de seguridad se restaura.

Almacenar copias de seguridad en un servidor FTP seguro

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

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

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

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

NOTA:

Virtual Edition está basado en Linux Debian Ubuntu x64.

Inicie sesión en VE con ddpsupport, y utilice el comando sudo para configurar la solución de copia de seguridad:

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

Contenido de copia de seguridad de las siguientes carpetas:



/opt/dell/vsftpd/files/backup (obligatorio)

/opt/dell/vsftpd/files/certificates (se recomienda encarecidamente)

/opt/dell/vsftpd/files/support (opcional)

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

Habilitar el acceso remoto a la base de datos

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

NOTA: Dell recomienda habilitar el acceso remoto a la base de datos solamente si es necesario.

- 1 En el menú *Configuración avanzada*, seleccione **Acceso remoto a la base de datos**.
- 2 Use la barra espaciadora para introducir una **X** en el campo Habilitar acceso remoto a la base de datos y seleccione **Aceptar**. Si la contraseña de la base de datos no se ha configurado aún, se mostrará un indicador para la contraseña de la base de datos.
- 3 Introduzca la contraseña de la base de datos.
- 4 Vuelva a introducir la contraseña de la base de datos.
Los componentes de la aplicación DDP se detienen automáticamente.

Habilitar la compatibilidad del servidor DMZ

Esta tarea se puede realizar en cualquier momento. No es necesario empezar a utilizar DDP Enterprise Server - VE. Se recomienda reiniciar los servicios cuando se realice un cambio de configuración.

- 1 En el menú *Configuración avanzada*, seleccione **Habilitar la compatibilidad del servidor DMZ**.
- 2 Use la barra espaciadora para introducir una **X** en el campo Habilitar la compatibilidad del servidor DMZ y seleccione **Aceptar**.

NOTA: Para utilizar Modo Proxy (modo DMZ), debe [instalar y configurar el modo Proxy](#).

DDP Enterprise Server - Tareas del administrador VE

Establecer o cambiar el idioma de terminal de DDP Enterprise Server - VE

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

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

Comprobar el estado del servidor

Para comprobar el estado de los servicios de DDP Enterprise Server - VE, en el menú principal, seleccione **Estado del servidor**.

La tabla a continuación describe cada uno de los servicios y sus funciones.

| Nombre | Descripción |
|--|--|
| Dell Message Broker | Bus de Enterprise Server |
| Dell Identity Server | Procesa las solicitudes de autenticación de dominios. |
| Dell Compatibility Server | Un servicio para administrar la arquitectura empresarial. |
| Dell Security Server | Proporciona un mecanismo para controlar comandos y comunicaciones con Active Directory. Se utiliza para establecer comunicación con Dell Policy Proxy. |
| Dell Compliance Reporter | Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías. |
| Dell Core Server | Un servicio para administrar la arquitectura empresarial. |
| Dell Core Server HA (Alta disponibilidad) | Un servicio de alta disponibilidad que permite una seguridad aumentada y rendimiento de conexiones HTTPS al administrar la arquitectura empresarial. |
| Dell Inventory Server | Procesa la cola de inventario. |
| Dell Forensic Server | Proporciona servicios web para la API forense. |
| Dell Policy Proxy | Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario. |

DDP Enterprise Server - VE supervisa y reinicia sus servicios, si es necesario.



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

Ver registros

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

Registro Syslog Registro Mail Registro Auth (SSH) Registro Postgres Registro Monitor

- Registros del sistema
 - Registro Syslog
 - Registro Mail
 - Registro Auth (SSH)
 - Registro Postgres
 - Registro Monitor
- Registros del servidor
 - Compatibility Server
 - Security Server
 - Message Broker
 - Core Server
 - Core Server HA
 - Compliance Reporter
 - Identity Server
 - Inventory Server
 - Forensic Server
 - Policy Proxy
- Registro Databasecustomizer

Abrir la interfaz de la línea de comandos

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

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

Generar un registro de instantáneas del sistema

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

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

Si el usuario ddpsupport está activado, Dell ProSupport puede podrá obtener el registro desde el servidor de DDP Enterprise Server - VE. Si el usuario de ddpsupport no está activado, póngase en contacto con Dell ProSupport. Para obtener más información, consulte [Póngase en contacto con Dell ProSupport](#).



Mantenimiento de DDP Enterprise Server - VE

Debe eliminar copias de seguridad de DDP Enterprise Server - VE innecesarias.

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

Solución de problemas de DDP Enterprise Server - VE

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

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



Tareas de configuración posteriores a la instalación

Después de la instalación, es posible que algunos componentes de su entorno necesiten ser configurados, en función de la solución de Dell Data Protection utilizada en su organización.

Configurar VE para Data Guardian

Para configurar VE para que admita Data Guardian, en la Remote Management Console VE, establezca la política de Cifrado de nube en Activado. Para activar el modo de documentos de Office protegidos de Data Guardian, establezca la política correspondiente.

Para obtener instrucciones sobre cómo instalar el cliente de Data Guardian, consulte la guía *Enterprise Edition Advanced installation Guide* (Guía de instalación avanzada de *Enterprise Edition*), *Enterprise Edition Basic installation Guide* (Guía de instalación básica de *Enterprise Edition*) o la guía Data Guardian (Guía del usuario de *Data Guardian*).

Instalar y configurar EAS Management para Mobile Edition

Para utilizar Mobile Edition, debe instalar y configurar EAS Management. Si no va a utilizar Mobile Edition, ignore esta sección.

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.
- Es necesaria una conexión de red a DDP Enterprise Server - VE.
- Tenga a mano el nombre de host o la dirección IP de DDP Enterprise Server - VE.
- Microsoft Message Queuing (MSMQ) ya debe estar instalado y configurado en el servidor que aloja el entorno de Exchange. De lo contrario, instale MSMQ 4.0 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>

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 Mobile Edition, 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 **Instalaren** la pantalla Listo para iniciar 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 Mobile Edition, 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 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 usar 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 **Instalaren** la pantalla Listo para iniciar 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 la utilidad de configuración de EAS.

2 Haga clic en **Configuración** para configurar los valores de EAS Management.

3 Introduzca la siguiente información:

Nombre de host de DDP Enterprise Server - VE

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

Seleccione la casilla de verificación 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, pero aun así le muestra la 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.

Pasos para realizar después del proceso de implementación



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

En sus servidores de buzones de Exchange

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

Nombre de host de DDP Enterprise Server - VE

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

Desmarque 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.
- 5 Haga clic en **Salir** cuando haya terminado.

Habilitar comprobación de cadenas de confianza del administrador

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

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

Para habilitar la validación de confianza SSL/TLS, en el equipo cliente, cambie el valor de la entrada de registro siguiente a 0:

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

DisableSSLCertTrust=REG_DWORD (32-bit):0



Tareas del administrador de la Remote Management Console VE

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 sesión en el servidor de Remote Management Console Enterprise Server.
- 2 Inicie sesión en el servidor de Remote Management Console Enterprise Server e inicie sesión con credenciales de usuario de dominio. Haga clic en "?" en la esquina superior derecha de la Remote Management Console para iniciar la *Ayuda del administrador de Dell Data Protection*. Aparecerá la página *Introducción*. Haga clic en **Agregar dominios**.

A modo de línea base, hay políticas que están establecidas para su organización, pero es posible que necesiten ser modificadas según sus requisitos específicos, de la forma siguiente (la concesión de licencias y autorizaciones rige todas las activaciones):

- Se cifran los equipos Windows
- Se cifran los equipos que tienen unidades de cifrado automático
- Se cifran los equipos Windows que tienen hardware acelerador de cifrado
- No se habilita la administración de BitLocker
- No se habilita Advanced Threat Protection
- Se ha habilitado Threat Protection



- No se cifran los soportes externos
- No se cifran los dispositivos conectados a puertos
- Data Guardian está activado
- No se habilita Mobile Edition

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

Confirmar políticas

Confirmar políticas cuando haya finalizado la instalación.

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

- 1 En el panel izquierdo, haga clic en **Administración** > **Confirmar**.
- 2 Introduzca una descripción del cambio en el campo Comentario.
- 3 Haga clic en **Confirmar políticas**.



Puertos de la solución

La siguiente tabla describe cada componente y su función.

| Nombre | Puerto predeterminado | Descripción | Necesario para |
|---|-----------------------|--|----------------|
| Compliance Reporter | HTTP(S)/8084 | Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías. Un componente de DDP Enterprise Server - VE. | Informes |
| Remote Management Console | HTTPS/8443 | Consola de administración y centro de control para implementación en toda la empresa. Un componente de DDP Enterprise Server - VE. | Todo |
| Core Server | HTTPS/8888 | Administra el flujo de políticas, las licencias y el registro para Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat 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 DDP Enterprise Server - VE. | Todo |
| Core Server HA (Alta disponibilidad) | HTTPS/8888 | Un servicio de alta disponibilidad que permite seguridad y rendimiento aumentados de conexiones HTTPS con la Remote Management Console, la Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat Protection. Un componente de DDP Enterprise Server - VE. | Todo |
| Security Server | HTTPS/8443 | Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, los productos de Data Guardian y la comunicación de SED-PBA. Un componente de DDP Enterprise Server - VE. | Todo |
| Compatibility Server | TCP/1099 (cerrado) | Un servicio para administrar la arquitectura empresarial. Recopila y almacena los datos de inventario iniciales durante la activación y los datos de políticas durante las migraciones. Procesa datos en función de los grupos de usuarios de este servicio. Un componente de DDP Enterprise Server - VE. | Todo |
| Message Broker Service | TCP/61616 | Administra la comunicación entre los servicios de DDP Enterprise Server - VE. Organiza la información de políticas creada por el | Todo |



| Nombre | Puerto predeterminado | Descripción | Necesario para |
|--------------------------------|---|--|--|
| | y STOMP/61613 (cerrado, o si está configurado para DMZ, 61613 está abierto) | Compatibility Server para poner en cola el policy proxy. Un componente de DDP Enterprise Server - VE. | |
| Identity Server | HTTPS/8445 | Procesa las solicitudes de autenticación de dominios, incluida la autenticación del SED Manager. Requiere una cuenta de Active Directory. Un componente de DDP Enterprise Server - VE. | Todo |
| Forensic Server | HTTPS/8448 | Permite a los administradores que tienen privilegios adecuados obtener las claves de cifrado de la Remote Management Console, para utilizarlas en desbloques de datos o tareas de descifrado. Un componente de DDP Enterprise Server - VE. | API forense |
| Inventory Server | 8887 | Procesa la cola de inventario. Un componente de DDP Enterprise Server - VE. | Todo |
| Policy Proxy | TCP/ 8000/8090 | Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario. Un componente de DDP Enterprise Server - VE. | Enterprise Edition para Mac Enterprise Edition para Windows Mobile Edition |
| LDAP | 389/636, 3268/3269 RPC - 135, 49125+ | Puerto 3268: este puerto se utiliza para solicitudes destinadas específicamente para el catálogo general. Las solicitudes LDAP enviadas al puerto 3268 se pueden utilizar para buscar objetos en todo el bosque. Sin embargo, solo se pueden devolver los atributos marcados para la replicación en el catálogo general. Por ejemplo, el departamento de un usuario no se puede devolver si utiliza el puerto 3268 ya que este atributo no se replica en el catálogo general. Puerto 389: este puerto se utiliza para solicitar información desde la controladora de dominio local. Las solicitudes LDAP enviadas al puerto 389 se pueden utilizar para buscar objetos solo en el dominio de inicio del catálogo general. Sin embargo, la aplicación solicitante puede obtener todos los atributos para dichos objetos. Por ejemplo, se puede utilizar una solicitud al puerto 389 para obtener un departamento de usuario. | Todo |
| Autenticación del cliente | HTTPS/8449 | Permite a los servidores cliente autenticarse frente a DDP Enterprise Server - VE. | Server Encryption |
| Aviso de devolución de llamada | HTTP/8446 | Permite insertar un aviso de devolución de llamada en cada archivo de Office protegidos, al ejecutar Data Guardian en el modo de Office protegido. | Data Guardian |

| Nombre | Puerto predeterminado | Descripción | Necesario para |
|----------------------------|-----------------------|--|---|
| Advanced Threat Prevention | HTTPS/TCP/443 | Comunicación de cliente si se utiliza Advanced Threat Prevention | Advanced Threat Prevention |
| EAS Device Manager | N/A | Habilita funciones a través del aire. Se instala en Exchange Client Access Server. | Administración Exchange ActiveSync de dispositivos móviles. |
| EAS Mailbox Manager | N/A | El agente del buzón que está instalado en Exchange Mailbox Server. | Administración Exchange ActiveSync de dispositivos móviles. |

Sincronización de hora NTP: TCP y UDP/123 (para obtener más información, consulte <https://help.ubuntu.com/lts/serverguide/NTP.html>.)

