Introducción

Servicios de implementación de Dell Data Security

Notas, precauciónes y advertencias

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

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

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

Introducción

2019 - 06

Rev. A01

Contenido

1

Fases de implementación

El proceso de implementación básico incluye estas fases:

- Realizar una Revisión de los requisitos y puesta en marcha
- Completar una Lista de comprobación de preparación - Implementación inicial o Lista de comprobación de preparación - Actualización/Migración
- Instalar o actualizar/migrar ***uno*** de los siguientes:
  - ***Servidor de administración de seguridad***
    - Administración centralizada de dispositivos
    - Aplicación de Windows que se ejecute en un entorno físico o virtual.
  - ***Servidor virtual de administración de seguridad***
    - Administración centralizada de hasta 3.500 dispositivos
    - Se ejecuta en un entorno virtualizado

    Para obtener instrucciones de instalación/migración para Dell Server, consulte la *guía de migración e instalación de* Servidor de administración de seguridad o la *guía de instalación e inicio rápido de Servidor virtual de administración de seguridad*. Para obtener estos documentos, consulte los documentos de Dell Data Security Server.
- Configurar la política inicial
  - ***Servidor de administración de seguridad***: consulte las *tareas administrativas, la guía de migración e instalación de Servidor de administración de seguridad*, disponibles en support.dell.com, y la ayuda *AdminHelp* que está disponible en la consola de administración
  - ***Servidor virtual de administración de seguridad***: consulte las *tareas administrativas de la consola de administración*, *la guía de inicio rápido e instalación de Servidor virtual de administración de seguridad*, disponibles en support.dell.com, y la ayuda *AdminHelp* que está disponible en la consola de administración
- Empaquetado de cliente

  En caso de que necesite información acerca de los requisitos de cliente y los documentos de instalación de software, seleccione los documentos pertinentes según su implementación:
  - *Guía de instalación básica de Encryption Enterprise* o *Guía de instalación avanzada de Encryption Enterprise*
  - *Guía de instalación básica de Endpoint Security Suite Enterprise* o *Guía de instalación avanzada de Endpoint Security Suite Enterprise*
  - *Guía del administrador de Advanced Threat Prevention*
  - *Guía de instalación de Encryption Personal*
  - *Guía del administrador de Encryption Enterprise para Mac*
  - *Guía del administrador de Endpoint Security Suite Enterprise para Mac*
  - *Guía del administrador de Dell Data Guardian*
  - *Guía del usuario de Dell Data Guardian*

    Para obtener estos documentos, consulte los documentos de clientes Dell Data Security.
- Participe en la transferencia de conocimientos básicos de Dell Security Administrator
- Implementar las mejores prácticas
- Coordine el soporte de implementación o un piloto con Dell Client Services

Revisión de los requisitos y puesta en marcha

Antes de la instalación, es importante que entienda su entorno y los objetivos técnicos y empresariales de su proyecto para implementar correctamente Dell Data Security de modo que cumpla con dichos objetivos. Asegúrese de que tiene un entendimiento completo de los requisitos generales de seguridad de datos de su organización.

Las siguientes son preguntas comunes clave para ayudar al equipo de Dell Client Services a entender su entorno y requisitos:

1. ¿Cuál es el tipo de negocio de su organización (asistencia médica, etc.)?
2. ¿Qué requisitos de conformidad reglamentaria tiene (HIPAA/HITECH, PCI, etc.)?
3. ¿Cuál es el tamaño de su organización (número de usuarios, número de ubicaciones físicas, etc.)?
4. ¿Cuál es el número seleccionado de extremos para la implementación? ¿Tienen planes de ampliar por encima de este número en el futuro?
5. ¿Los usuarios tienen privilegios de administrador local?
6. ¿Qué datos y dispositivos necesita para administrar y cifrar (discos fijos locales, USB, etc.?
7. ¿Qué productos tiene pensado implementar?
   - Encryption Enterprise
     - Encryption (autorización de DE): Windows Encryption, Server Encryption, Medios externos de cifrado, SED Management, FDE, BitLocker Manager y Mac Encryption.
     - Medios externos de cifrado
   - Endpoint Security Suite Enterprise
     - Advanced Threat Prevention: con o sin servidor de seguridad del cliente opcional y protección web (autorización ATP)
     - Encryption (autorización de DE): Windows Encryption, Server Encryption, Medios externos de cifrado, SED Management, FDE, BitLocker Manager y Mac Encryption.
     - Medios externos de cifrado
   - Dell Data Guardian (derecho a CE)
8. ¿Qué tipo de conectividad de usuario admite su organización? Los tipos pueden incluir lo siguiente:
   - Solo conectividad de LAN local
   - Usuarios inalámbricos de Enterprise y/o basados en VPN
   - Usuarios desconectados/remotos (usuarios no conectados a la red directamente o mediante VPN durante periodos extendidos de tiempo)
   - Estaciones de trabajo sin dominio
9. ¿Qué datos necesita proteger en el extremo? ¿Qué tipo de datos tienen los usuarios típicos en el extremo?
10. ¿Qué aplicaciones de usuario pueden contener información sensible? ¿Cuáles son los tipos de archivo de la aplicación?
11. ¿Cuántos dominios tiene en su entorno? ¿Cuántos hay en el ámbito para el cifrado?
12. ¿A cuáles sistemas operativos y versiones de estos se dirige el cifrado?
13. ¿Tiene particiones de inicio alternativa configuradas en sus extremos?
    a. Partición de recuperación del fabricante
    b. Estaciones de trabajo de inicio doble

Documentos de cliente

En caso de que necesite información acerca de los requisitos de instalación, las versiones de sistema operativo compatibles, las unidades con autocifrado compatibles y las instrucciones para los clientes que desea implementar, consulte los documentos pertinentes que se indican a continuación.

Encryption Enterprise (Windows): consulte los documentos en www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

- *Guía de instalación avanzada de Encryption Enterprise*: guía de instalación, en la que se incluyen los parámetros y switches avanzados para realizar instalaciones personalizadas.
- *Guía del usuario de la consola de Dell Data Security*: instrucciones para usuarios.

Encryption Enterprise (Mac): consulte la *guía del administrador de Encryption Enterprise para Mac* en www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Incluye instrucciones de instalación e implementación.

Endpoint Security Suite Enterprise (Windows): consulte los documentos en www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Guía de instalación avanzada de Endpoint Security Suite Enterprise*: guía de instalación, en la que se incluyen los parámetros y switches avanzados para realizar instalaciones personalizadas.
- *Endpoint Security Suite EnterpriseAdvanced Threat Prevention*Administración de instrucciones, incluidas las recomendaciones de políticas, la identificación y la administración de amenazas, y la solución de problemas.
- *Guía del usuario de la consola de Dell Data Security*: instrucciones para usuarios.

Endpoint Security Suite Enterprise (Mac): consulte el documento enwww.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Guía del administrador de Endpoint Security Suite Enterprise para Mac*: guía de instalación

Dell Data Guardian: consulte los documentos en www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

- *Guía del administrador de Dell Data Guardian*: instrucciones de instalación, activación y operación.
- *Guía del usuario de Dell Data Guardian*: instrucciones de instalación, activación y operación para usuarios.

Para obtener información sobre las unidades con autocifrado compatibles, consulte https://www.dell.com/support/article/us/en/04/sln296720.

Documentos de servidor

En caso de que necesite información acerca de los requisitos de instalación, las versiones de sistema operativo compatibles y las configuraciones de Dell Server que piensa implementar, consulte los documentos pertinentes que se indican a continuación.

Servidor de administración de seguridad

- Consulte la *Guía de instalación y migración de Servidor de administración de seguridad* en

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

  O bien

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

  O bien

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

Servidor virtual de administración de seguridad

- Consulte la *Guía de inicio rápido y guía de instalación de Servidor virtual de administración de seguridad* en

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

  O bien

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

  O bien

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

3

Lista de comprobación de preparación - Implementación inicial

En función del Dell Server que esté implementando, utilice la lista de verificación adecuada para asegurarse de que cumple con todos los requisitos previos antes de comenzar la instalación de Dell Encryption, Endpoint Security Suite Enterprise o Data Guardian.

- Lista de verificación de Security Management Server
- Lista de verificación de Security Management Server Virtual

Lista de verificación de la implementación inicial de Servidor de administración de seguridad

¿Se ha completado la limpieza del entorno de Prueba de concepto (si se aplica)?

- ☐ Se ha realizado una copia de seguridad y desinstalado la aplicación y la base de datos de la prueba de concepto (si utiliza el mismo servidor) antes de la interacción de instalación con Dell. Para obtener más instrucciones sobre la desinstalación, consulte https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us.
- ☐ Se han decodificado todos los terminales de producción utilizados durante la evaluación de la prueba de concepto o se han descargado los paquetes de clave. Para obtener más información sobre los clientes que desea implementar, consulte Documentos de cliente.

NOTA:
Todas las implementaciones nuevas deben comenzar con una base de datos nueva y la instalación recién realizada del software Encryption, Endpoint Security Suite Enterprise o Data Guardian. Dell Client Services no realizará una implementación nueva mediante un entorno POC. Se deberá descifrar o reconstruir cualquier terminal cifrado durante una Prueba de concepto (POC) antes de la interacción de instalación con Dell.

¿Los servidores cumplen con las especificaciones de hardware necesarias?

- ☐ Consulte Diseño de arquitectura de Dell Security Management Server.

¿Los servidores cumplen con las especificaciones de software necesarias?

- ☐ Windows Server 2012 R2 (Standard o Datacenter), 2016 (Standard o Datacenter), o Windows Server 2019 (Standard o Datacenter) está instalado. Estos sistemas operativos se pueden instalar en componentes de hardware físicos o virtuales.
- ☐ Se ha instalado Windows Installer 4.0 o posterior.
- ☐ Se ha instalado .NET Framework 4.5.
- ☐ Se ha instalado Microsoft SQL Native Client 2012, si utiliza SQL Server 2012 o SQL Server 2016. Si está disponible, se utilizará SQL Native Client 2014.

  NOTA: SQL Express no es compatible con una implementación de producción de Servidor de administración de seguridad.

- ☐ Se deshabilitó o configuró Windows Firewall para admitir puertos (de entrada) 8000, 8050, 8081, 8084, 8888, 61613.
- ☐ Hay conectividad disponible entre Servidor de administración de seguridad y Active Directory (AD) en los puertos 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (entrada a AD).
- ☐ UAC se deshabilita antes de la instalación en Windows Server 2012 R2 cuando se instala en C:\Program Files. El servidor debe reiniciarse para que el cambio tenga efecto. (consulte Panel de control de Windows > Cuentas de usuario).
  - Windows Server 2012 R2 - el instalador deshabilita UAC.
  - Windows Server 2016 R2 - el instalador deshabilita UAC.

  NOTA: El UAC ya no se deshabilitará de manera forzada, a menos que se especifique un directorio protegido para el directorio de instalación.

¿Se han creado correctamente las cuentas de mantenimiento?

- ☐ Cuenta de mantenimiento con acceso de solo lectura a AD (LDAP) - es suficiente con la cuenta de usuario de dominio/usuario básico.
- ☐ La cuenta de servicio debe tener derechos de administrador local en los servidores de aplicaciones Servidor de administración de seguridad.
- ☐ Para utilizar la autenticación de Windows para la base de datos, se deberá establecer una cuenta de servicios de dominio con derechos de administrador del sistema. 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.
- ☐ Para utilizar la autenticación SQL, la cuenta SQL utilizada debe tener derechos de administrador del sistema en 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.

¿Se ha descargado el software?

Descárguelo desde el sitio web de Dell Support.

- ☐ Las descargas de software de cliente de Dell Data Security y Servidor de administración de seguridad se localizan 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/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

  En la página del producto http://www.dell.com/support

  1 Seleccione **Controladores y descargas**.
  2 En la lista de sistemas operativos, seleccione el sistema operativo correcto para el producto que está descargando. Por ejemplo, para descargar Dell Enterprise Server, seleccione **una de las opciones de Windows Server.**
  3 Bajo el título de software adecuado, seleccione **Descargar archivo**.
- ☐ Si compró Encryption o Endpoint Security Suite Enterprise incluido en la caja, el software se puede enviar a la computadora de destino a través de Dell Digital Delivery.

O bien

Descárguelo del sitio de transferencia de archivos (CFT) Dell Data Security

- ☐ El software se encuentra en https://ddpe.credant.com en la carpeta **Descargas de software**.

¿Están disponibles el archivo de licencia y la clave de instalación?

- ☐ La clave de licencia se incluye en el correo electrónico original junto con las credenciales de FTP. Consulte el ejemplo de correo electrónico de notificación del cliente. Esta clave también se incluye en la descarga de la aplicación desde http://www.dell.com/support y https://ddpe.credant.com.
- ☐ El archivo de licencia corresponde a un archivo XML ubicado en la carpeta **Licencias de cliente** del sitio FTP.

NOTA:
Si ha adquirido sus licencias en la caja, no se necesita un archivo de licencia. La autorización se descarga automáticamente de Dell tras la activación de cualquier cliente Data Guardian, Encryption, Enterprise o Endpoint Security Suite Enterprise nuevo.

¿Se ha creado la base de datos?

- ☐ (Opcional) Se crea una base de datos nueva en un servidor compatible: consulte Requisitos y arquitectura en la *Guía de migración e instalación de Servidor de administración de seguridad*. El instalador de Servidor de administración de seguridad crea una base de datos durante la instalación si aún no se ha creado ninguna.
- ☐ Se han otorgado derechos **db_owner** al usuario de la base de datos de destino.

¿Se ha creado un alias DNS para Servidor de administración de seguridad o Policy Proxies con Split DNS para tráfico externo e interno?

Se recomienda que cree varios alias DNS para obtener escalabilidad. Esto le permitirá agregar servidores adicionales posteriormente o separar componentes de la aplicación sin que sea necesaria la actualización del cliente.

- ☐ Se crean alias DNS, si se desea. Alias DNS sugeridos:
  - Servidor de administración de seguridad: dds.<domain.com>
  - Servidor de front-end: dds-fe.<domain.com>

NOTA:
Split-DNS admite a un usuario del mismo nombre de DNS de manera interna y externa. Esto implica que se puede proporcionar internamente dds.<domain.com> como un c-name interno y dirigirlo a Dell Security Management Server (back-end) y, de manera externa, proporcionar un a-record para dds.<domain.com> y reenviar los puertos pertinentes (consulte Puertos para Security Management Server) al servidor de front-end. Es posible aprovechar el round-robin de DNS o un equilibrio de carga para distribuir la carga a los distintos front-ends (en caso de que existan varios).

¿Plan para los certificados SSL?

- ☐ Tenemos una Entidad emisora de certificados (CA) que se puede utilizar para firmar certificados y que todas las estaciones de trabajo en el entorno confían en ella **o** tenemos previsto comprar un certificado firmado utilizando una Entidad emisora de certificados pública, como VeriSign o Entrust. Si utiliza una autoridad de certificación pública, informe al ingeniero de Dell Client Services. El Certificado contiene la Cadena completa de confianza (Raíz e Intermedio) con las firmas clave públicas y privadas.
- ☐ Los Nombres alternativos de sujeto (SAN) en la solicitud de certificado coinciden con todos los alias de DNS que se han dado a cada servidor utilizado para la instalación de Dell Server. No es válido para los comodines ni las solicitudes de certificado autofirmado.
- ☐ El certificado se genera en un formato .pfx.

¿Se han identificado y comunicado los requisitos de control de cambio a Dell?

- ☐ Envíe cualquier requisito específico de Control de cambio para la instalación de Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services antes de la interacción de la instalación. Estos requisitos pueden incluir cambios en los servidores de la aplicación, base de datos y estaciones de trabajo del cliente.

¿Se ha preparado el hardware de prueba?

- ☐ Prepare al menos tres equipos con la imagen del equipo corporativo para que se utilicen para pruebas. Dell recomienda que **no** utilice computadoras de producción en la realización de pruebas. Las computadoras de producción se pueden utilizar durante un piloto de producción después de que se hayan definido y probado las políticas de cifrado mediante el plan de prueba que Dell proporcionó.

Lista de verificación de la implementación inicial de Servidor virtual de administración de seguridad

¿Se ha completado la limpieza del entorno de Prueba de concepto (si se aplica)?

- ☐ Se ha realizado una copia de seguridad y desinstalado la aplicación y la base de datos de la prueba de concepto (si utiliza el mismo servidor) antes de la interacción de instalación con Dell. Para obtener más instrucciones sobre la desinstalación, consulte https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us

- ☐ Se han decodificado todos los terminales de producción utilizados durante la evaluación de la prueba de concepto o se han descargado los paquetes de clave. Para obtener más información sobre los clientes que desea implementar, consulte Documentos de cliente.

NOTA:
Todas las implementaciones nuevas deben comenzar con una base de datos nueva y la instalación recién realizada del software Encryption, Endpoint Security Suite Enterprise o Data Guardian. Dell Client Services no realizará una implementación nueva mediante un entorno POC. Se deberá descifrar o reconstruir cualquier terminal cifrado durante una Prueba de concepto (POC) antes de la interacción de instalación con Dell.

¿Se han creado correctamente las cuentas de mantenimiento?

- ☐ Cuenta de mantenimiento con acceso de solo lectura a AD (LDAP) - es suficiente con la cuenta de usuario de dominio/usuario básico.

¿Se ha descargado el software?

- ☐ Las descargas de software de cliente de Dell Data Security y Servidor de administración de seguridad se localizan 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/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

  En la página del producto http://www.dell.com/support

  1. Seleccione **Controladores y descargas**.
  2. En la lista de sistemas operativos, seleccione el sistema operativo correcto para el producto que está descargando. Por ejemplo, para descargar Dell Enterprise Server, seleccione **una de las opciones de Windows Server.**

3 Bajo el título de software adecuado, seleccione **Descargar archivo**.

- ☐ Si compró Encryption o Endpoint Security Suite Enterprise incluido en la caja, el software se puede enviar a la computadora de destino a través de Dell Digital Delivery.

¿Hay archivos de licencia disponibles?

- ☐ El archivo de licencia corresponde a un archivo XML ubicado en la carpeta **Licencias de cliente** del sitio ddpe.credant.com.

NOTA:
Si ha adquirido sus licencias en la caja, no se necesita un archivo de licencia. La autorización se descarga automáticamente de Dell tras la activación de cualquier cliente Encryption o Endpoint Security Suite Enterprise nuevo.

¿Los servidores cumplen con las especificaciones de hardware necesarias?

- ☐ Consulte Diseño de arquitectura de Security Management Server Virtual.

¿Se creó un alias DNS para Security Management Server Virtual o Policy Proxies con Split DNS para tráfico externo e interno?

Se recomienda que cree varios alias DNS para obtener escalabilidad. Esto le permitirá agregar servidores adicionales posteriormente o separar componentes de la aplicación sin que sea necesaria la actualización del cliente.

- ☐ Se crean alias DNS, si se desea. Alias DNS sugeridos:
  - Servidor de administración de seguridad: dds.<domain.com>
  - Servidor de front-end: dds-fe.<domain.com>

NOTA:
Split-DNS admite a un usuario del mismo nombre de DNS de manera interna y externa. Esto implica que se puede proporcionar internamente dds.<domain.com> como un c-name interno y dirigirlo a Dell Security Management Server (back-end) y, de manera externa, proporcionar un a-record para dds.<domain.com> y reenviar los puertos pertinentes (consulte Puertos para Security Management Server Virtual) al servidor de front-end. Es posible aprovechar el round-robin de DNS o un equilibrio de carga para distribuir la carga a los distintos front-ends (en caso de que existan varios).

¿Plan para los certificados SSL?

- ☐ Tenemos una Entidad emisora de certificados (CA) que se puede utilizar para firmar certificados y que todas las estaciones de trabajo en el entorno confían en ella **o** tenemos previsto comprar un certificado firmado utilizando una Entidad emisora de certificados pública, como VeriSign o Entrust. Si utiliza una Entidad emisora de certificados pública, informe a Dell Client Services Engineer.

¿Se han identificado y comunicado los requisitos de control de cambio a Dell?

- ☐ Envíe cualquier requisito específico de Control de cambio para la instalación de Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services antes de la interacción de la instalación. Estos requisitos pueden incluir cambios en los servidores de la aplicación, base de datos y estaciones de trabajo del cliente.

¿Se ha preparado el hardware de prueba?

- ☐ Prepare al menos tres equipos con la imagen del equipo corporativo para que se utilicen para pruebas. Dell recomienda que **no** utilice computadoras de producción en la realización de pruebas. Las computadoras de producción se pueden utilizar durante un

piloto de producción después de que se hayan definido y probado las políticas de cifrado mediante el plan de prueba que Dell proporcionó.

Lista de comprobación de preparación - Actualización/Migración

Esta lista de verificación se aplica solo a Servidor de administración de seguridad.

NOTA:
Actualizar Servidor virtual de administración de seguridad en el menú Configuración básica en el terminal de Dell Server. Para obtener más información, consulte las *guías de inicio rápido y de instalación de Servidor virtual de administración de seguridad*.

Utilice la siguiente lista para asegurarse de que cumple con todos los requisitos antes de comenzar la actualización de Encryption, Endpoint Security Suite Enterprise o Data Guardian.

¿Los servidores cumplen con las especificaciones de software necesarias?

- ☐ Windows Server 2012 R2 (Standard o Datacenter), Windows Server 2016 (Standard o Datacenter) o Windows Server 2019 (Standard o Datacenter) está instalado. De manera alternativa, se puede instalar un entorno virtualizado.
- ☐ Se ha instalado Windows Installer 4.0 o posterior.
- ☐ Se ha instalado .NET Framework 4.5.
- ☐ Se ha instalado Microsoft SQL Native Client 2012, si utiliza SQL Server 2012 o SQL Server 2016. Si está disponible, se utilizará SQL Native Client 2014.

  NOTA: SQL Express no es compatible con Servidor de administración de seguridad.
- ☐ Se deshabilitó o configuró Windows Firewall para admitir puertos (de entrada) 8000, 8050, 8081, 8084, 8443, 8888, 61613.
- ☐ Hay conectividad disponible entre Servidor de administración de seguridad y Active Directory (AD) en los puertos 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (entrada a AD).
- ☐ UAC se deshabilita antes de la instalación en Windows Server 2012 R2 cuando se instala en C:\Program Files. El servidor debe reiniciarse para que el cambio tenga efecto. (consulte Panel de control de Windows > Cuentas de usuario).
  - Windows Server 2012 R2 - el instalador deshabilita UAC.
  - Windows Server 2016 R2 - el instalador deshabilita UAC.

¿Se han creado correctamente las cuentas de mantenimiento?

- ☐ Cuenta de mantenimiento con acceso de solo lectura a AD (LDAP) - es suficiente con la cuenta de usuario de dominio/usuario básico.
- ☐ La cuenta de servicio debe tener derechos de administrador local en los servidores de aplicaciones Servidor de administración de seguridad.
- ☐ Para utilizar la autenticación de Windows para la base de datos, se deberá establecer una cuenta de servicios de dominio con derechos de administrador del sistema. 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.

- ☐ Para utilizar la autenticación SQL, la cuenta SQL utilizada debe tener derechos de administrador del sistema en 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.

¿Se ha hecho copia de seguridad de la base de datos y de todos los archivos necesarios?

- ☐ Se realiza 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.
- ☐ Asegúrese de que se hace copia de seguridad de todos estos archivos más críticos, que 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

¿Están disponibles el archivo de licencia y la clave de instalación?

- ☐ La clave de licencia se incluye en el correo electrónico original con las credenciales CFT - consulte Ejemplo de correo electrónico de notificación del cliente. Esta clave también se incluye en la descarga de la aplicación desde http://www.dell.com/support y https://ddpe.credant.com.
- ☐ El archivo de licencia corresponde a un archivo XML ubicado en la carpeta **Licencias de cliente** del sitio CFT.

NOTA:
Si ha adquirido sus licencias en la caja, no se necesita un archivo de licencia. La autorización se descarga automáticamente de Dell tras la activación de cualquier cliente Encryption o Endpoint Security Suite Enterprise nuevo.

¿Se ha descargado software nuevo y existente de Dell Data Security?

Descárguelo del sitio de transferencia de archivos (CFT) Dell Data Security

- ☐ El software se encuentra en https://ddpe.credant.com en la carpeta **Descargas de software**.
- ☐ Si compró Data Guardian, Encryption Enterprise o Endpoint Security Suite Enterprise incluido en la caja (OTB), se puede proveer opcionalmente el software a través de Dell Digital Delivery. De forma alternativa, se puede descargar el software desde www.dell.com/support o ddpe.credant.com, respectivamente.

¿Tiene suficientes licencias de extremo?

Antes de la actualización, asegúrese de que tiene suficientes licencias de cliente para cubrir todos los terminales de su ambiente. Si actualmente sus instalaciones exceden la cantidad de licencias, comuníquese con su representante de ventas de Dell antes de realizar la actualización o migración. Dell Data Security realiza la validación de la licencia y se impiden las activaciones si no hay licencias disponibles.

- ☐ Tengo suficientes licencias para cubrir mi entorno.

¿Los registros de DNS se documentan?

- ☐ Valide la documentación y la preparación para actualización de los registros de DNS en caso de que se reemplace un componente de hardware.

¿Plan para los certificados SSL?

- ☐ Tenemos una Entidad emisora de certificados (CA) que se puede utilizar para firmar certificados y que todas las estaciones de trabajo en el entorno confían en ella **o** tenemos previsto comprar un certificado firmado utilizando una Entidad emisora de certificados pública, como VeriSign o Entrust. Si utiliza una autoridad de certificación pública, informe al ingeniero de Dell Client Services. El Certificado contiene la Cadena completa de confianza (Raíz e Intermedio) con las firmas clave públicas y privadas.

- ☐ Los Nombres alternativos de sujeto (SAN) en la Solicitud de certificado coinciden con todos los alias DNS que se han dado a cada servidor utilizado para la instalación de Dell Enterprise Server. No se aplica a comodines ni a solicitudes de certificado autofirmadas.

- ☐ El certificado se genera en un formato .pfx.

¿Se han identificado y comunicado los requisitos de control de cambio a Dell?

- ☐ Envíe cualquier requisito específico de Control de cambio para la instalación de Encryption, Endpoint Security Suite Enterprise o Data Guardian a Dell Client Services antes de la interacción de la instalación. Estos requisitos pueden incluir cambios en los servidores de la aplicación, base de datos y estaciones de trabajo del cliente.

¿Se ha preparado el hardware de prueba?

- ☐ Prepare al menos tres equipos con la imagen del equipo corporativo para que se utilicen para pruebas. Dell recomienda que **no** utilice computadoras de producción en la realización de pruebas. Las computadoras de producción se pueden utilizar durante un piloto de producción después de que se hayan definido y probado las políticas de cifrado mediante el plan de prueba que Dell proporcionó.

5

Arquitectura

Esta sección describe las recomendaciones de diseño de la arquitectura para la implementación de Dell Data Security. Seleccione Dell Server que implementará:

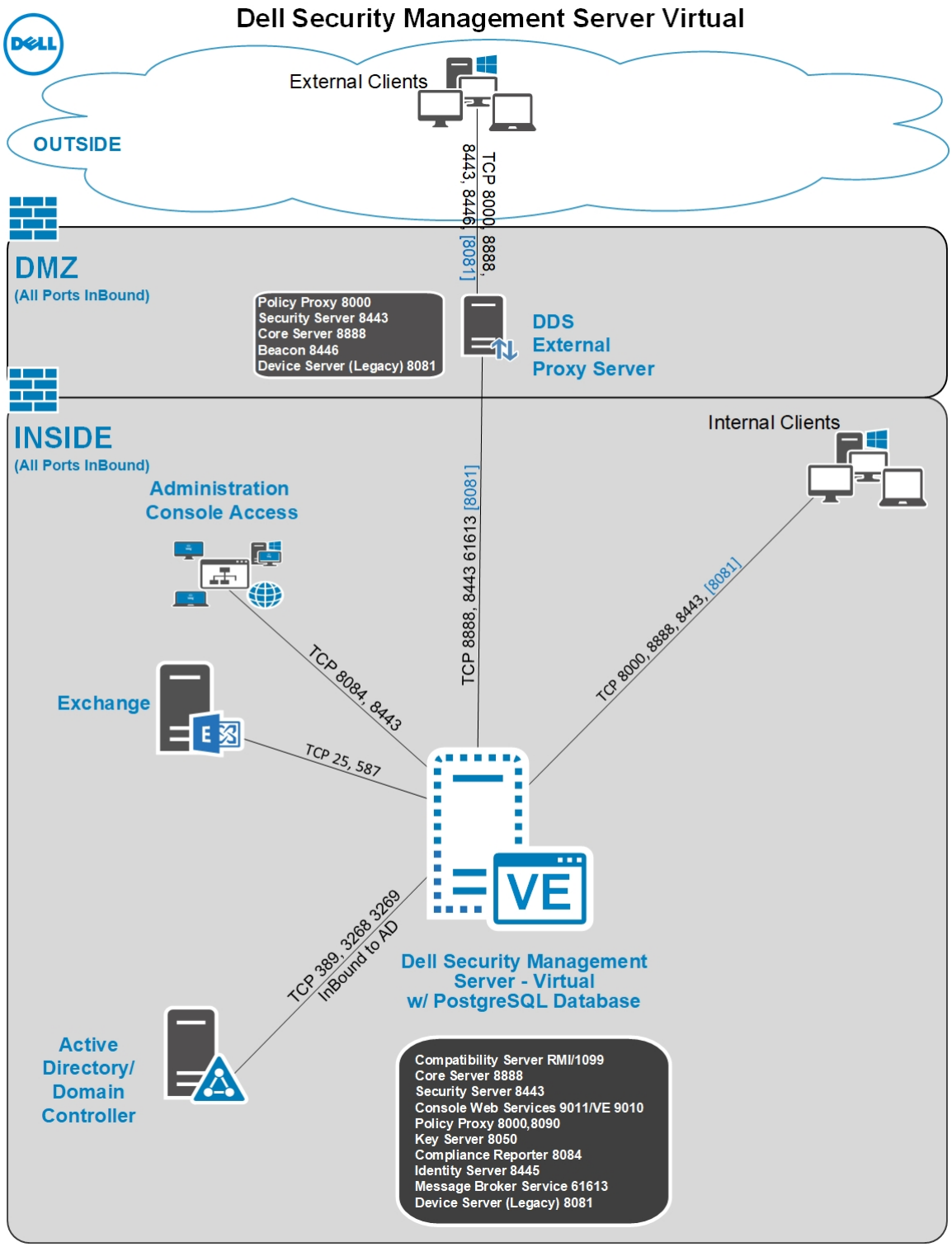
- Diseño de arquitectura de Security Management Server
- Diseño de arquitectura de Security Management Server Virtual

Diseño de arquitectura de Security Management Server Virtual

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

Componentes de la arquitectura

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



Puertos

La siguiente tabla describe cada componente y su función.

Nombre	Puerto predeterminado	Descripción
Compliance Reporter	HTTP(S)/ 8084	Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías.
Consola de administración	HTTPS/ 8443	Consola de administración y centro de control para implementación en toda la empresa.
Core Server	HTTPS/ 8887 (cerrado)	Administra el flujo de políticas, las licencias y el registro para Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat Prevention. Procesa los datos de inventario para que los utilice Compliance Reporter y la consola de administración. Recopila y almacena datos de autenticación. Controla el acceso basado en roles.
Core Server HA (Alta disponibilidad)	HTTPS/ 8888	Un servicio de alta disponibilidad que permite seguridad y rendimiento aumentados para las conexiones HTTPS con la consola de administración, la autenticación previa al arranque, SED Management, FDE, BitLocker Manager, Threat Protection y Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, los productos de Data Guardian y la comunicación de SED-PBA.
Compatibility Server	TCP/ 1099 (cerrado)	Un servicio para administrar la arquitectura empresarial. Recopila y almacena los datos de inventario iniciales durante la activación y los datos de políticas durante las migraciones. Procesa datos según los grupos de usuario.
Message Broker Service	TCP/ 61616 (cerrado) y STOMP/ 61613 (cerrado, o si está configurado para DMZ, 61613 está abierto)	Maneja la comunicación entre los servicios de Dell Server. Organiza la información de políticas que se crea con el Compatibility Server para poner en cola el Policy Proxy.
Identity Server	8445 (cerrado)	Maneja las solicitudes de autenticación de dominio, incluida la autenticación de SED Management.
Forensic Server	HTTPS/ 8448	Permite a los administradores que tienen los privilegios adecuados obtener las claves de cifrado de la consola de administración para utilizarlas en los desbloqueos de datos o las tareas de descifrado. Se necesita para la API de Forensic.
Inventory Server	8887	Procesa la cola de inventario.
Policy Proxy	TCP/ 8000	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario. Se necesita para Encryption Enterprise (Windows y Mac)

Nombre	Puerto predeterminado	Descripción
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Puerto 389: este puerto se utiliza para solicitar información desde la controladora de dominio local. Las solicitudes LDAP enviadas al puerto 389 se pueden utilizar para buscar objetos solo en el dominio de inicio del catálogo general. Sin embargo, la aplicación solicitante puede obtener todos los atributos para dichos objetos. Por ejemplo, se puede utilizar una solicitud al puerto 389 para obtener un departamento de usuario. Puerto 3268: este puerto se utiliza para solicitudes destinadas específicamente para el catálogo general. Las solicitudes LDAP enviadas al puerto 3268 se pueden utilizar para buscar objetos en todo el bosque. Sin embargo, solo se pueden devolver los atributos marcados para la replicación en el catálogo general. Por ejemplo, el departamento de un usuario no se puede devolver si utiliza el puerto 3268 ya que este atributo no se replica en el catálogo general.
Autenticación del cliente	HTTPS/ 8449	Permite la autenticación de los servidores cliente en Dell Server. Se necesita para Server Encryption
Aviso de devolución de llamada	HTTP/TCP 8446	En un servidor front-end, permite insertar un aviso de devolución de llamada en cada archivo de Office protegido, al ejecutar Data Guardian en el modo de Office protegido.

Diseño de arquitectura de Security Management Server

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

Componentes de la arquitectura

A continuación, se muestran configuraciones de hardware sugeridas que son adecuadas para la mayoría de los ambientes.

Servidor de administración de seguridad

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

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

Proxy Server

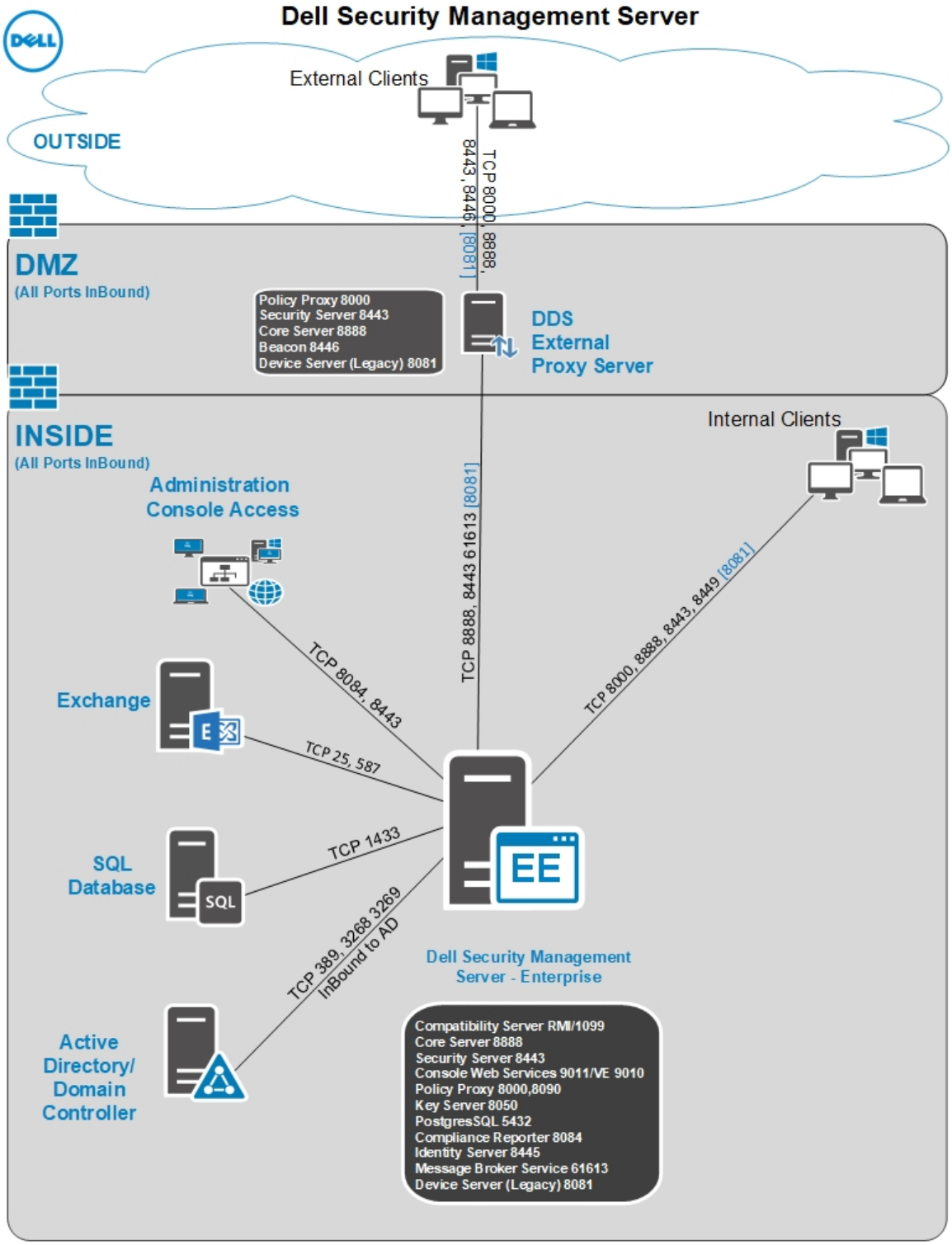
- Sistema operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Equipo virtual/físico
- CPU: 2 núcleos
- RAM: 8 GB
- Unidad C: 20 GB de espacio disponible en el disco para los registros

Especificaciones de hardware de SQL Server

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

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

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



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

Puertos

La siguiente tabla describe cada componente y su función.

Nombre	Puerto predeterminado	Descripción
Compliance Reporter	HTTP(S)/ 8084	Proporciona una vista amplia del entorno para realizar informes de cumplimiento y auditorías.
Consola de administración	HTTP(S)/ 8443	Consola de administración y centro de control para implementación en toda la empresa.
Core Server	HTTPS/ 8888	Administra el flujo de políticas, las licencias y el registro para Autenticación previa al inicio, SED Management, BitLocker Manager, Threat Protection y Advanced Threat Prevention. Procesa los datos de inventario para que los utilice Compliance Reporter y la consola de administración. Recopila y almacena datos de autenticación. Controla el acceso basado en roles.
Device Server	HTTPS/ 8081	Permite activaciones y la recuperación de la contraseña. Un componente de Servidor de administración de seguridad. Se necesita para Encryption Enterprise (Windows y Mac)
Security Server	HTTPS/ 8443	Se comunica con Policy Proxy; administra la recuperación de clave forense, las activaciones de clientes, Data Guardian, la comunicación de SED-PBA y Active Directory para la autenticación o la reconciliación, incluida la validación de identidades para la autenticación en la consola de administración. Requiere el acceso de base de datos SQL.
Compatibility Server	TCP/ 1099	Un servicio para administrar la arquitectura empresarial. Recopila y almacena los datos de inventario iniciales durante la activación y los datos de políticas durante las migraciones. Procesa datos según los grupos de usuario.
Message Broker Service	TCP/ 61616 y STOMP/ 61613	Maneja la comunicación entre los servicios de Dell Server. Organiza la información de políticas que se crea con el Compatibility Server para poner en cola el Policy Proxy. Requiere el acceso de base de datos SQL.
Key Server	TCP/ 8050	Negocia, autentica y cifra una conexión cliente utilizando las API de Kerberos. Requiere acceso a la base de datos SQL para extraer los datos clave.
Policy Proxy	TCP/ 8000	Proporciona una ruta de comunicación de red para entregar actualizaciones de políticas de seguridad y actualizaciones de inventario.
LDAP	TCP/ 389/636 (controladora de dominio local), 3268/3269 (catálogo global) TCP/	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.

Nombre	Puerto predeterminado	Descripción
	135/ 49125+ (RPC)	Puerto 3268: este puerto se utiliza para solicitudes destinadas específicamente para el catálogo general. Las solicitudes LDAP enviadas al puerto 3268 se pueden utilizar para buscar objetos en todo el bosque. Sin embargo, solo se pueden devolver los atributos marcados para la replicación en el catálogo general. Por ejemplo, el departamento de un usuario no se puede devolver si utiliza el puerto 3268 ya que este atributo no se replica en el catálogo general.
Base de datos de Microsoft SQL	TCP/ 1433	El puerto de SQL Server predeterminado es 1433 y se asignan a los puertos clientes un valor aleatorio entre 1024 y 5000.
Autenticación del cliente	HTTPS/ 8449	Permite la autenticación de los servidores cliente en Dell Server. Se necesita para Server Encryption.
Aviso de devolución de llamada	HTTP/TCP 8446	Permite insertar un aviso de devolución de llamada en cada archivo de Office protegidos, al ejecutar Data Guardian en el modo de Office protegido.

6

Prácticas recomendadas para SQL Server

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

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

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

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

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

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

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

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

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

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

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

Ejemplo de correo electrónico de notificación del cliente

Después de la adquisición de Dell Data Security, recibirá un correo electrónico de DellDataSecurity@Dell.com. A continuación, encontrará un ejemplo del correo electrónico, que incluye sus credenciales de CFT e información de clave de licencia.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - U.S. & Canada Only
- Outside the U.S., click here for a list of numbers

Need Support? CHAT NOW! Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options