Dell Encryption Key Manager 3.0
Guía de implementación

Notas, precauciones y avisos

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.

PRECAUCIÓN: un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos si no se siguen las instrucciones.

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

2011 – 12

Rev. A00

Tabla de contenido

1

Información general

Dell Encryption Key Manager (EKM) 3.0 es una utilidad de cifrado que protege los datos almacenados en cartuchos de cinta LTO mediante la administración de claves de cifrado para las soluciones de automatización de cintas Dell, incluidas las series ML y TL PowerVault. EKM 3.0 administra el ciclo de vida de las claves de cifrado de cinta, incluida la generación, distribución, administración y eliminación.

En esta guía se describe cómo instalar y configurar Dell Encryption Key Manager 3.0 (EKM 3.0), así como realizar operaciones básicas en él. Dell recomienda que lea este documento antes de instalar EKM 3.0.

En esta guía se proporciona información sobre lo siguiente:

- Los requisitos de hardware y software para EKM 3.0
- La instalación y desinstalación de EKM 3.0 en plataformas Windows y Linux
- La configuración de EKM 3.0
- Las operaciones básicas en EKM 3.0
- La migración de EKM 2.X durante la instalación de EKM 3.0 y la combinación de EKM 2.X en una instalación de EKM 3.0 configurada
- Preguntas frecuentes, información de solución de problemas, mensajes de error comunes e información sobre el contacto de la asistencia técnica

NOTA: EKM 3.0 se basa en IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, pero se ha personalizado para admitir entornos de bibliotecas de cintas Dell mediante la selección del subconjunto adecuado de las funciones de TKLM para las cintas.

Para obtener información sobre el uso de EKM 3.0 que no se incluye en esta guía, consulte la documentación de TKLM, que incluye lo siguiente:

- IBM Tivoli Key Manager 2.0 *Guía de inicio rápido*
- IBM Tivoli Key Manager 2.0 *Guía de instalación y configuración*
- IBM Tivoli Key Manager 2.0 *Descripción general del producto/guía de escenarios*

Para obtener información sobre cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Algunas pantallas y funciones que se cubren en la documentación de IBM TKLM no están activadas en Dell EKM 3.0. EKM 3.0 contiene solo el subconjunto de funciones necesarias para las bibliotecas de cintas de Dell PowerVault.

NOTA: Para información sobre el uso y la configuración recomendado de Dell EKM 3.0, consulte la sección de recomendaciones del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

NOTA: Para obtener la información más reciente sobre las mejoras de las funciones y las correcciones de errores, consulte las notas de la versión en: **support.dell.com/manuals**. Vaya a **Software → Systems Management (Administración de sistemas) → Dell Encryption Key Manager** .

Requisitos de hardware y software

Requisitos de hardware de servidor

Los requisitos mínimos de hardware para el Key Management Server (el hardware en el que se instalará EKM 3.0) son los siguientes:

- CPU: 2,3 GHz
- Memoria: memoria ECC de 4GB
- Almacenamiento de disco disponible (para la instalación de EKM 3.0 y el almacenamiento de claves típico): 5 GB

NOTA: Si el sistema en el que instala EKM 3.0 tienes 24 o más CPUs, consulte las notas de publicación de EKM 3.0 para obtener información sobre cómo actualizar EKM 3.0 tras completar la instalación. Para obtener acceso a las notas de publicación de EKM 3.0, vaya a **support.dell.com/manuals** y vaya a **Software → Systems Management(Administración de sistemas) → Dell Encryption Key Manager**.

Requisitos del explorador

EKM 3.0 admite los exploradores siguientes:

- Microsoft Internet Explorer, versión 7.0
- Microsoft Internet Explorer, versión 8.0, modo de Vista de compatibilidad
- Firefox versión 3.0.x (EKM 3.0 no admite Firefox versión 3.5 y superior).

NOTA: JavaScript debe estar activado para que funcionen todas las características de EKM 3.0. Consulte la documentación del explorador para obtener instrucciones sobre la activación de JavaScript.

Requisitos del sistema operativo

EKM 3.0 admite los sistemas operativos siguientes:

- Windows Server 2003 R2 con Service Pack 2, 32 bits y 64 bits, ediciones Standard y Enterprise
- Windows Server 2008 con Service Pack 2, 32 bits y 64 bits, edición Standard y Enterprise
- Windows Server 2003 R2, ediciones Standard y Enterprise
- Red Hat Enterprise Linux (RHEL) 4.X, Advanced Server (AS), 32 bits
- Red Hat Enterprise Linux (RHEL) 5.X, 32 bits y 64 bits
- SUSE Linux Enterprise Server (SLES) 10 con Service Pack 4, 64 bits
- SUSE Linux Enterprise Server (SLES) 11 con Service Pack 1, 64 bits

NOTA: EKM 3.0 no admite VMware o Microsoft Hyper-V Server.

NOTA: Para obtener información sobre los requisitos y las limitaciones de establecer la configuración de un servidor principal o secundario, consulte Configuración de los servidores principal y secundario de EKM 3.0.

NOTA: EKM 3.0 realiza comprobaciones sobre los requisitos previos del sistema antes de realizar la instalación. Para obtener información, consulte Comprobaciones sobre los requisitos previos del sistema.

2

Instalación de EKM 3.0

En este capítulo se describe cómo instalar EKM 3.0 en Windows y Linux.

NOTA: Si actualmente utiliza EKM 2.X, Dell recomienda conservar la infraestructura actual (servidores, sistemas operativos, bibliotecas de cinta, etc. que están bajo la protección de EKM 2.X), a menos que esté experimentando problemas.

EKM 3.0 no admite el uso de máquinas virtuales como hosts. Si utiliza una máquina virtual como host de EKM 2.X, deberá seguir utilizando EKM 2.X o migrar a un servidor físico.

NOTA: Si tiene previsto migrar su versión de EKM 2.X a EKM 3.0, consulte Migración de Encryption Key Manager (EKM) versión 2.X durante la instalación de EKM 3.0 antes de comenzar la instalación de EKM 3.0.

NOTA: Dell recomienda que instale EKM 3.0 en un servidor físico dedicado que no se utiliza para ningún otro servicio. De este modo, garantizará el rendimiento de EKM 3.0 y los tiempos de respuesta no se verán afectados por otras aplicaciones que se ejecuten en el mismo servidor físico.

PRECAUCIÓN: EKM 3.0 solo admite la instalación directa desde el soporte de EKM 3.0. No copie el contenido del soporte de EKM 3.0 en el disco duro.

NOTA: Los procedimientos que se describen en este capítulo requieren conocimientos de nivel de administrador.

Preparación para la instalación de EKM 3.0 en Microsoft Windows

En este capítulo se describen los pasos previos a la instalación de Dell Encryption Key Manager 3.0 en Microsoft Windows.

NOTA: El proceso de instalación tarda aproximadamente 45 minutos. No apague el sistema hasta que se complete el proceso de instalación.

NOTA: Debe estar conectado como **Administrador** para instalar EKM 3.0.

NOTA: Si no desea usar una contraseña compleja para la base de datos, desactive la opción **La contraseña debe cumplir con los requisitos de complejidad** en el sistema operativo antes de insertar el soporte de instalación de EKM 3.0.

1. Inserte el disco de instalación EKM 3.0 para Microsoft Windows en el sistema en el que desee instalar EKM 3.0.
2. Si el sistema está configurado para autoejecutarse al insertar un DVD, espere un momento hasta que aparezca el instalador. De lo contrario, vaya a la unidad de DVD y haga doble clic en la unidad de DVD o en **install.exe** en la raíz de la unidad de DVD.

   Aparecerá la pantalla **Welcome** (Bienvenida) del asistente de instalación de EKM 3.0.

NOTA: Si desea instalar EKM 3.0 a través de un recurso compartido de red, no utilice una ruta de acceso con el formato siguiente: **\\<*ip_address*>*EKM_3.0_share***. En cambio, asigne el recurso compartido a una letra de unidad. En Explorador de Windows, utilice **Herramientas** → **Conectar a unidad de red** para establecer la ruta de acceso de instalación en **<*shared_drive_letter*>:\<*EKM_3.0_media*>**.

Proceda a Procedimiento de instalación de EKM 3.0.

Preparación para la instalación de EKM 3.0 en Red Hat Enterprise Linux

En este capítulo se describen los pasos previos a la instalación de Dell Encryption Key Manager 3.0 en Red Hat Enterprise Linux.

NOTA: El proceso de instalación tarda aproximadamente 45 minutos. No apague el sistema hasta que se complete el proceso de instalación.

Para preparase para la instalación de EKM 3.0, realice los pasos siguientes:

1. Inserte el disco de instalación EKM 3.0 adecuado para el sistema operativo en el que desee instalar EKM 3.0.
2. Si el sistema está configurado para autoejecutar cuando se inserte un DVD, espere un momento hasta que aparezca el instalador. De lo contrario, abra una sesión de terminal con acceso a la raíz y vaya a la carpeta en la que está montado el DVD de EKM 3.0. Escriba **./autorun.sh** y presione **Intro**.

NOTA: Si SELinux está instalado y activado, desactívelo antes de iniciar la instalación. Consulte Comprobaciones sobre los requisitos previos del sistema.

NOTA: Con frecuencia, los sistemas operativos Red Hat tienen el bit **noexec** configurado para desactivar la ejecución de binarios en los sistemas de archivos montados. Si el bit **noexec** del DVD ROM montado se ha configurado en **disable** (desactivado), el instalador de EKM 3.0 no se iniciará desde el DVD. Para iniciar el instalador de EKM 3.0 desde el DVD, realice los pasos siguientes:

a) Abra una sesión de terminal con acceso a la raíz.
b) Desmonte el DVD de EKM 3.0.
c) Vuelva a montar el DVD de EKM 3.0 en modo de **read-only** (solo lectura) con **noexec** desactivado. Para ello, ejecute los comandos siguientes:

```
mkdir /media/dellmedia mount /dev/<EKM 3.0 device><space>/media/dellmedia
cd /media/dellmedia
```

d) Para ejecutar el instalador, escriba **./autorun.sh** y presione **Intro**.

Aparecerá la pantalla **Welcome** (Bienvenida) del asistente de instalación de EKM 3.0.

Proceda a Procedimiento de instalación de EKM 3.0.

Preparación para la instalación de EKM 3.0 en SUSE Linux Enterprise Server

En este capítulo se describen los pasos previos a la instalación de Dell Encryption Key Manager 3.0 en SUSE Linux Enterprise Server.

NOTA: El proceso de instalación tarda aproximadamente 45 minutos. No apague el sistema hasta que se complete el proceso de instalación.

Para preparase para la instalación de EKM 3.0, realice los pasos siguientes:

1. Inserte el disco de instalación EKM 3.0 adecuado para el sistema operativo del equipo en el que desee instalar EKM 3.0.
2. Si el sistema está configurado para autoejecutar cuando se inserte un DVD, espere un momento hasta que aparezca el instalador. De lo contrario, abra una sesión de terminal con acceso a la raíz y vaya a la carpeta en la que está montado el DVD de EKM 3.0. Escriba **./autorun.sh** y presione **Intro**.

   Aparecerá la pantalla **Welcome** (Bienvenida) del asistente de instalación de EKM 3.0.

NOTA: Si SELinux está instalado y activado, desactívelo antes de iniciar la instalación.

3. Abra el puerto 50000. Para ello, realice los pasos siguientes:
   a) Vaya a **Computer (Ordenador)** → **Places (Lugares)** → **File System (Sistema de archivos)**.
   b) Haga doble clic en **etc**.
   c) Haga doble clic en **Services** (Servicios).
   d) En el archivo **Services** (Servicios), cambie **50000/tcp** y **50000/udp** a **50100/tcp** y **50100/udp**.
   e) Haga clic en **Save** (Guardar).

Proceda a Procedimiento de instalación de EKM 3.0.

Realización del procedimiento de instalación de EKM 3.0

En este capítulo se describe cómo instalar EKM 3.0.

NOTA: El proceso de instalación tarda aproximadamente 45 minutos. No apague el sistema hasta que se complete el proceso de instalación.

NOTA: Si instala EKM 3.0 en un servidor que se utilizará como un servidor secundario de EKM 3.0, las contraseñas deben ser las mismas que las que ha utilizado para la instalación del servidor principal de EKM 3.0.

1. En la pantalla **Welcome** (Bienvenida) del asistente de instalación de EKM 3.0, haga clic en **Next** (Siguiente).
   Se abre la ventana del **License Agreement** (Contrato de licencia).
2. Seleccione el botón de radio para aceptar las condiciones del contrato de licencia.
3. Haga clic en **Next** (Siguiente).

NOTA: El instalador de EKM 3.0 realiza las comprobaciones de los requisitos previos del sistema y verifica que este último cumple con los requisitos mínimos. Asimismo, configura EKM 3.0 para el sistema.

Si aparece un mensaje de error, consulte Comprobaciones sobre los requisitos previos del sistema.

Aparece la ventana **Reuse Installation Profile** (Volver a utilizar el perfil de instalación).

4. *Si instala EKM 3.0 por primera vez*, deje la casilla **Reuse an EKM 3.0 installation profile** (Volver a utilizar un perfil de instalación de EKM 3.0) desactivada.
   Si está reinstalando EKM 3.0 o está instalando EKM 3.0 en el servidor secundario y desea utilizar el perfil de instalación que ha guardado de una instalación anterior, realice los pasos siguientes:
   a) Seleccione la casilla **Reuse an EKM 3.0 installation profile** (Volver a utilizar un perfil de instalación de EKM 3.0). Se activará el campo **File Location** (Ubicación del archivo).
   b) Haga clic en **Choose** (Elegir) y vaya al perfil de instalación que ha creado al instalar y configurar EKM 3.0 anteriormente (por ejemplo, **E:\EKM_config.txt** en Windows o **/tmp/ekm_config** en Linux).
      Puede utilizar una unidad extraíble o un recurso compartido de red para transferir el perfil de instalación desde la ubicación en la que lo ha guardado.

NOTA: El perfil de instalación rellena todos los campos de entrada, excepto los de las contraseñas, en la GUI de instalación con la misma información que ha utilizado en una instalación anterior. Si utiliza un perfil de instalación, deberá volver a introducir todas las contraseñas.

NOTA: Si está instalando EKM 3.0 en un servidor secundario, deberá volver a utilizar el perfil de instalación del servidor principal de EKM 3.0 para asegurarse de que los parámetros de entrada sean los mismos.

5. Haga clic en **Next** (Siguiente).
   Aparecerá la pantalla **Database** (Base de datos). En ella, creará una cuenta de administrador de bases de datos DB2 de EKM.

NOTA: Esta pantalla y las dos pantallas subsiguientes crean una cuenta diferente. Anote todos los nombres de usuario y contraseñas que cree para estas cuentas.

6. El valor predeterminado del campo **Database Location** (Ubicación de la base de datos) es una ubicación establecida. Dell recomienda conservar la ubicación predeterminada. Se trata de la ubicación en la que el instalador instalará el software DB2 de EKM 3.0.
7. En el campo **Database User Name** (Nombre de usuario de base de datos), introduzca un nombre de usuario que cumpla los criterios siguientes:

   - Solo incluir letras en minúsculas (a–z), números (0–9) y el carácter de guión bajo (_).
   - No puede tener una longitud superior a ocho caracteres
   - No puede comenzar con "ibm," "sys", "sql" o un número
   - No puede comenzar o terminar con un carácter de guión bajo (_)
   - No puede ser una palabra reservada para DB2 (por ejemplo, "users", "admins," "guests", "public" y "local") ni una palabra reservada para SQL.
   - No puede ser el nombre de usuario de un usuario existente del sistema

   Se trata del ID de la cuenta de administrador de bases de datos DB2 de EKM 3.0. EKM 3.0 crea una cuenta de usuario local en el sistema con este nombre de usuario.
8. En el campo **Database Password** (Contraseña de base de datos), introduzca una contraseña para la cuenta de administrador de bases de datos DB2 de EKM. En el campo **Confirm Database Password** (Confirmar contraseña de base de datos), vuelva a escribir la contraseña.

NOTA: Todas las contraseñas distinguen entre mayúsculas y minúsculas.

NOTA: Dell recomienda el uso de contraseñas seguras para todas las cuentas de usuario de EKM 3.0.

9. En el campo **Database Data Drive** (Unidad de datos de base de datos), introduzca la ubicación de la unidad de la base de datos. Se trata de la ubicación en la que se almacenarán los datos DB2 de EKM 3.0. En Windows, introduzca una letra de unidad y dos puntos (:). En Linux, introduzca una ubicación de carpeta, por ejemplo, **/home/ekmdb2**.
10. En el campo **Database Name** (Nombre de base de datos), introduzca un nombre para la base de datos DB2 de EKM 3.0.
11. El valor predeterminado del campo **Database Port** (Puerto de base de datos) es **50010** en Windows y **50000** en Linux.

    Todos los puertos que EKM 3.0 utiliza y establece durante el proceso de instalación de EKM 3.0 se preconfiguran con las direcciones de puerto recomendadas. Dell recomienda firmemente que utilice estas direcciones de puerto. Si tiene previsto utilizar un servidor secundario y cambia una dirección de puerto al instalar EKM 3.0, la dirección de puerto debe ser la misma que para los servidores principal y secundario de EKM 3.0.

NOTA: Para instalar EKM 3.0, todos los puertos que se utilizan durante el proceso de instalación deben estar abiertos. Compruebe que están abiertos:

Para comprobar que los puertos están abiertos en Windows:

a. Vaya a: **<*root*>:\Windows\System32\drivers\etc**.
b. Abra el archivo de texto **Services** (Servicios).
c. Revise el archivo y confirme que el número de puerto que desee utilizar en el campo **Database Port** (Puerto de base de datos) está disponible. Si lo está, no figurará en la lista.

Para comprobar que los puertos están abiertos en Linux:

a. Abra el archivo **/etc/services**.
b. Revise el archivo y confirme que el número de puerto que desee utilizar en el campo **Database Port** (Puerto de base de datos) está disponible. Si lo está, no figurará en la lista.

12. Haga clic en **Next** (Siguiente).

    Aparece la ventana **EKM Administrator** (Administrador de EKM). En ella, creará la cuenta de administrador (superusuario) de EKM 3.0, que se utilizará para crear usuarios y grupos nuevos, así como asignar los permisos correspondientes.

13. En el campo **Administrator Username** (Nombre de usuario de administrador), introduzca el nombre de usuario del administrador de EKM 3.0 (puede ser cualquier nombre, excepto **tklmadmin**).
14. En el campo **Password** (Contraseña), introduzca una contraseña para la cuenta de administrador de EKM. En el campo **Confirm Password** (Confirmar contraseña), vuelva a escribir la contraseña.
15. Haga clic en **Next** (Siguiente).

    Aparecerá la pantalla **Encryption Manager**. En ella, creará la cuenta de EKM 3.0 Encryption Manager (TKLMAdmin), que es la cuenta de usuario habitual y se utiliza para la administración diaria de claves. El campo **TKLMAdmin Username** (Nombre de usuario TKLMAdmin) contiene el texto **tklmadmin**, que es el nombre obligatorio de EKM Encryption Manager.
16. En el campo **TKLMAdmin Password** (Contraseña de TKLMAdmin), introduzca una contraseña para la cuenta de EKM 3.0 Encryption Manager. En el campo **TKLMAdmin Confirm Password** (Confirmar contraseña de TKLMAdmin), vuelva a escribir la contraseña.
17. El valor predeterminado de **EKM Port** (Puerto de EKM) es **16310** en Windows y Linux. Este es el puerto recomendado. Haga clic en **Next** (Siguiente).

NOTA: Si otro servicio está utilizando el puerto proporcionado, el instalador de EKM 3.0 le solicitará que seleccione un puerto diferente. Utilice el comando **netstat** para determinar los puertos que están en uso y seleccione un puerto disponible. Registre el número de puerto, ya que lo utilizará para obtener acceso al portal de EKM 3.0.

Aparecerá la pantalla **Migration** (Migración) que se utiliza para migrar de EKM 2.X a EKM 3.0.

Si tiene una versión de EKM 2.X que desea migrar a EKM 3.0, debe migrarla ahora. Consulte Migración de Encryption Key Manager (EKM) versión 2.X durante la instalación de EKM 3.0.

NOTA: Solo es posible migrar una versión EKM 2.X que se ha utilizado para crear claves.

Si no dispone de una versión de EKM 2.X para migrar a EKM 3.0:

a) Deje la casilla **Migrate from EKM 2.X to EKM 3.0** (Migrar de EKM 2.X a EKM 3.0) desactivada y haga clic en **Next** (Siguiente).

   Aparecerá una ventana emergente.

b) Si ha optado por no migrar una versión de EKM 2.X, haga clic en **Yes** (Sí) en la ventana emergente y confirme que no migrará una versión de EKM 2.X.

   Aparece la pantalla **Configuration Summary** (Resumen de la configuración).

18. En la pantalla **Configuration Summary** (Resumen de la configuración), seleccione la casilla **Save profile** (Guardar perfil).

    Se activa el campo **File Directory** (Directorio de archivos).

NOTA: Dell recomienda guardar el perfil de instalación en caso de que sea necesario volver a instalar EKM 3.0 en una situación de recuperación tras un desastre. Un perfil de instalación guardado es necesario para crear un servidor secundario de EKM 3.0.

NOTA: Dell recomienda utilizar una unidad extraíble como la ubicación. En dicho caso, deberá insertar la unidad antes de hacer clic en **Next** (Siguiente). La unidad extraíble debe permanecer insertada hasta que finalice la instalación. De manera opcional, puede guardar el archivo en una ubicación de la unidad local y copiarlo en la unidad extraíble más adelante.

NOTA: La ruta que introduzca en este campo debe incluir un nombre de usuario. No introduzca solo un nombre de carpeta. La ruta de acceso de archivo a la carpeta hasta el nombre de usuario debe existir, pero el nombre de archivo que se utiliza para la instalación de perfil no debe existir.

19. En el campo **File Directory** (Directorio de archivos), introduzca la ubicación y el nombre de archivo del perfil de instalación que está creando o haga clic en **Choose** (Elegir) y seleccione una ubicación; a continuación, introduzca un nombre de archivo.

    Se trata de la ubicación en la que desea guardar el perfil de instalación y el nombre con el que lo desea guardar.

EKM 3.0 guarda el perfil de instalación una vez finalizada la instalación de EKM 3.0. Si utiliza una configuración de servidor principal/secundario, deberá utilizar el perfil de instalación del servidor principal de EKM 3.0 durante la instalación del servidor secundario de EKM 3.0 para rellenar automáticamente los campos de entrada de la instalación.

De manera opcional, si está reinstalando en el mismo servidor y desea utilizar los mismos campos, puede utilizar este perfil de instalación para rellenar automáticamente los campos de entrada de instalación.

NOTA: Dell recomienda capturar o imprimir la pantalla **Configuration Summary** (Resumen de la configuración) para referencia futura.

20. En la pantalla **Configuration Summary** (Resumen de la configuración), haga clic en **Next** (Siguiente).

    Aparece la pantalla **Installation Summary** (Resumen de la instalación).
21. Revise la información de la pantalla **Installation Summary** (Resumen de la instalación).
22. Haga clic en **Install** (Instalar).

NOTA: El proceso de instalación tarda aproximadamente 45 minutos. No apague el sistema hasta que se complete el proceso de instalación.

NOTA: Si tiene previsto configurar un servidor secundario de EKM 3.0, no instale EKM 3.0 en el servidor secundario hasta que se haya completado la instalación del servidor principal de EKM 3.0.

23. Una vez finalizada la instalación, haga clic en **Done** (Listo).

NOTA: Si ha migrado una versión de EKM 2.X a una instancia de EKM 3.0 recién instalada, Dell recomienda firmemente que cree una copia de seguridad de EKM 3.0 para asegurarse de que no se pierdan las claves nuevas. Consulte Creación de una copia de seguridad de la clasificación de claves.

NOTA: Si está reinstalando EKM 3.0 y la instalación falla debido a una desinstalación incompleta, realice la desinstalación manualmente. Consulte Desinstalación manual de EKM 3.0 en Windows.

3

Configuración de los servidores principal y secundario de EKM 3.0

En este capítulo se describe cómo instalar, utilizar y desinstalar EKM 3.0 en los servidores principal y secundario.

PRECAUCIÓN: Para evitar la posible pérdida de datos debido a un fallo del servidor de EKM 3.0, Dell recomienda utilizar una configuración de servidor principal y secundario de EKM 3.0. Esta configuración proporciona redundancia en el caso de que el servidor principal de EKM 3.0 esté fuera de servicio o no esté disponible.

NOTA: No es posible tener un servidor principal de EKM 3.0 y un servidor secundario de EKM 2.X o viceversa.

Instalación de EKM 3.0 en el servidor principal

Durante la instalación de EKM 3.0 en el servidor principal, debe seleccionar la opción para guardar el perfil de instalación. Cuando la instalación de EKM 3.0 en el servidor principal se haya completado, copie el perfil de instalación guardado en una unidad extraíble o un recurso compartido de servidor. Consulte Instalación de EKM 3.0.

Uso de EKM 3.0 en el servidor principal

El servidor principal de EKM 3.0 es donde se realizan todas las tareas de administración de claves de cifrado. De manera predeterminada, el servidor principal de EKM 3.0 se establece en **Automatically accept all new device requests for communication** (Aceptar automáticamente todas las nuevas solicitudes de dispositivo para la comunicación). Consulte Configuración de EKM 3.0 para aceptar dispositivos que contactan a EKM 3.0 para obtener claves para obtener información sobre cómo ver o configurar esta opción. Dell recomienda crear una copia de seguridad periódicamente del servidor principal de EKM 3.0. Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad.

Si el servidor principal de EKM 3.0 ha de reemplazarse por el motivo que sea, instale EKM 3.0 en un nuevo servidor físico mediante el perfil de instalación de la instalación original principal de EKM 3.0. Restaure el nuevo servidor principal de EKM 3.0 con la copia de seguridad más reciente y, a continuación, actualice todos los servicios para que se comuniquen con el nuevo servidor principal de EKM 3.0 para procesar sus solicitudes de clave. Consulte la guía del usuario de la biblioteca de cintas para obtener información sobre cómo cambiar la dirección IP del servidor de EKM 3.0 que se utiliza para solicitudes de clave. Para buscar la guía del usuario, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Instalación de EKM 3.0 en el servidor secundario

NOTA: No instale EKM 3.0 en el servidor secundario hasta que se haya completado la instalación del servidor primario de EKM 3.0.

El sistema en el que está instalado EKM 3.0 como servidor secundario debe tener la misma versión de sistema operativo que la instalada en el servidor EKM 3.0 primario. EKM 3.0 no admite la combinación de sistemas operativos entre el servidor primario y el secundario.

Instale EKM 3.0 en el servidor secundario según el procedimiento en Instalación de EKM 3.0. Utilice el perfil de instalación guardado al instalar EKM 3.0 en el servidor primario. Deberá introducir manualmente las mismas contraseñas que las que utilizó al instalar EKM 3.0 en el servidor primario.

Uso de EKM 3.0 en el servidor secundario

El servidor secundario de EKM 3.0 se utiliza para ofrecer redundancia en el caso de que el servidor principal EKM 3.0 esté fuera de servicio o no disponible.

Utilice la copia de seguridad creada en el servidor principal de EKM 3.0 para realizar la operación de restauración en el servidor secundario de EKM 3.0 periódicamente para mantener el servidor princiapl y el secundario EKM 3.0 sincronizados. Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad.

De manera predeterminada, el servidor secundario de EKM 3.0 también está establecido en **Automatically accept all new device requests for communication** (Aceptar automáticamente todas las nuevas solicitudes de dispositivo para la comunicación). Dell recomienda cambiar este valor a **Only accept manually added devices for communication** (Aceptar solamente dispositivos agregados manualmente para la comunicación). De este modo, el servidor secundario de EKM 3.0 no procesará claves a nuevos dispositivos que no estén agregados al servidor principal de EKM 3.0. Consulte Configuración de EKM 3.0 para aceptar dispositivos que contactan a EKM 3.0 para obtener claves para obtener detalles sobre cómo ver o configurar esta opción.

Si el servidor principal de EKM 3.0 está fuera de servicio o no disponible temporalmente, deberá realizar la operación de restauración en el servidor secundario de EKM 3.0 utilizando la última copia de seguridad creada en el servidor principal de EKM 3.0.

NOTA: Cuando el servidor principal de EKM 3.0 está fuera de servicio o no disponible y se utiliza el servidor secundario de EKM 3.0 para procesar las solicitudes de clave de los dispositivos, Dell recomienda no realizar tareas de administración u operativas en el servidor secundario de EKM 3.0.

Desinstalación de EKM 3.0 de los servidores principal y secundario

Para conocer el procedimiento de desinstalación de EKM 3.0 de los servidores principal y secundario, consulte Desinstalación de EKM 3.0.

4

Creación de copias de seguridad y restauración a partir de una copia de seguridad

Puede realizar una copia de seguridad en cualquier momento. Esto crea un archivo de copia de seguridad que contiene la clasificación de claves, que contiene dispositivos y claves.

Las copias de seguridad no contienen grupos de dispositivos, usuarios o grupos de usuarios. La base de datos de DB2 contiene estos elementos.

Puede realizar una restauración a partir de una copia de seguridad en cualquier momento.

NOTA: Si no se crea una copia de seguridad de las claves, estas no se procesarán. Si las claves no están disponibles para su procesamiento, fallarán los trabajos de copia de seguridad cifrados.

Creación de una copia de seguridad de la clasificación de claves

En este capítulo se describe cómo crear una copia de seguridad de la clasificación de claves.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager** → **Backup and Restore** (Copia de seguridad y restauración).

   Aparecerá la pantalla **Backup and Restore** (Copia de seguridad y restauración).
3. Haga clic en **Browse** (Examinar) junto al campo **Backup repository location** (Ubicación del repositorio de copia de seguridad) y vaya a la carpeta en la que desee guardar el archivo de copia de seguridad (por ejemplo, **C:\EKM_Backup** en Windows o **/root/EKM_Backup** en Linux).

NOTA: La carpeta debe existir antes de iniciar el proceso de copia de seguridad, de lo contrario, la operación fallará. Si desea utilizar una carpeta nueva, deberá crearla antes de intentar crear una copia de seguridad.

4. Haga clic en **Select** (Seleccionar) en la ventana emergente **Browse Directory** (Examinar directorio) para volver a la pantalla **Backup and Restore** (Copia de seguridad y restauración).
5. Haga clic en **Create Backup** (Crear copia de seguridad).

   Aparece la pantalla **Create Backup** (Crear copia de seguridad).
6. En el campo **Create password** (Crear contraseña) cree una contraseña para la copia de seguridad. Esta no debe tener menos de seis caracteres.

NOTA: Dell recomienda el uso de contraseñas seguras para todas las actividades relacionadas con EKM 3.0.

7. En el campo **Retype Password** (Volver a introducir contraseña), vuelva a introducir la contraseña.
8. (Opcional) En el campo **Backup description** (Descripción de la copia de seguridad), introduzca una descripción para el archivo de copia de seguridad. Si no especifica una descripción, se agregará una predeterminada al archivo de copia de seguridad.

NOTA: En algunas versiones de explorador, el campo de descripción predeterminada no se puede editar. Para obtener más información, consulte Problemas conocidos y las soluciones correspondientes.

9. Haga clic en **Create Backup** (Crear copia de seguridad).

   Aparecerá una ventana emergente de confirmación.

10. En la ventana emergente de confirmación, haga clic en **OK** (Aceptar). Se ejecutará el proceso de copia de seguridad.

NOTA: No utilice el sistema mientras se ejecuta el proceso de copia de seguridad. Si el contenido de EKM 3.0 aparece atenuado durante un tiempo prolongado, haga clic en el botón Actualizar del explorador.

11. Una vez creado el archivo de copia de seguridad, aparecerá una ventana emergente **Information** (Información) en la que se confirma que el archivo se ha creado correctamente. En esta ventana, haga clic en **OK** (Aceptar). El archivo de copia de seguridad creado se muestra en la tabla de la pantalla **Backup and Restore** (Copia de seguridad y restauración).
12. Haga clic en **Return home** (Volver al inicio) de la parte inferior de la pantalla.

    Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).

Restauración a partir de una copia de seguridad

Puede realizar una restauración a partir de una copia de seguridad. Puede utilizar una copia de seguridad para crear servidores de clave secundarios, así como volver a crear el servidor de EKM 3.0 en una situación de recuperación tres un desastre.

PRECAUCIÓN: Solo realice una restauración a partir de una copia de seguridad que se ha creado en el mismo sistema o en otro servidor de EKM 3.0 que se ha instalado mediante el mismo perfil de instalación. No puede realizar una restauración a partir de una copia de seguridad creada en un sistema diferente, utilizando detalles de instalación distintos.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager** → **Backup and Restore** (Copia de seguridad y restauración).

   Aparecerá la pantalla **Backup and Restore** (Copia de seguridad y restauración).
3. Seleccione la copia de seguridad a partir de la que desee realizar una restauración.
4. Haga clic en **Restore From Backup** (Restaurar a partir de copia de seguridad) de la parte superior de la tabla.

   Aparece la subventana **Restore From Backup** (Restaurar a partir de copia de seguridad).
5. Introduzca la contraseña del archivo de copia de seguridad.
6. Haga clic en **Restore Backup** (Restaurar copia de seguridad).

   Aparecerá una ventana emergente de confirmación.

PRECAUCIÓN: Las claves creadas después de la creación de la copia de seguridad se perderán junto con el acceso a los datos cifrados con dichas claves. Las claves perdidas o eliminadas no se pueden recuperar de ningún modo.

7. En la ventana emergente de confirmación, haga clic en **OK** (Aceptar).
8. Tras realizar una operación a partir de una copia de seguridad, deberá detener e iniciar manualmente el servidor de EKM 3.0. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.

5

Uso de EKM 3.0

En este capítulo se describen algunas operaciones básicas de EKM 3.0.

NOTA: EKM 3.0 se basa en IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, pero se ha personalizado para admitir entornos de bibliotecas de cintas Dell mediante la selección del subconjunto adecuado de las funciones de TKLM para las cintas.

Para obtener información sobre el uso de EKM 3.0 que no se incluye en esta guía, consulte la documentación de TKLM, que incluye lo siguiente:

- IBM Tivoli Key Manager 2.0 *Guía de inicio rápido*
- IBM Tivoli Key Manager 2.0 *Guía de instalación y configuración*
- IBM Tivoli Key Manager 2.0 *Descripción general del producto/guía de escenarios*

Para obtener información sobre cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Algunas pantallas y funciones que se cubren en la documentación de IBM TKLM no están activadas en Dell EKM 3.0. EKM 3.0 contiene solo el subconjunto de funciones necesarias para las bibliotecas de cintas de Dell PowerVault.

Conexión al portal de Encryption Key Manager 3.0

Para conectarse al portal de Encryption Key Manager 3.0, realice los pasos siguientes:

1. Abra un explorador e introduzca la dirección URL siguiente para abrir el portal de EKM 3.0:
   http://*<EKM 3.0_server_IP_address>*:*<EKM_3.0_port_number>*

   NOTA: El número de puerto especificado es el que ha proporcionado durante la instalación de EKM 3.0. El valor predeterminado es **16310**.

   Si desconoce el número de puerto, consulte lo siguiente:

   En Windows Consulte el valor de la propiedad **WC_defaulthost** en el archivo siguiente: ***<root>*:\Dell\EKM\profiles\TIPProfile\properties\portdef.props**.

   En Linux Consulte el valor de la propiedad **WC_defaulthost** en el archivo siguiente: **/opt/dell/ekm/profiles/TIPProfile/properties/portdef.props**.

   NOTA: Si aparece un mensaje de error en el que se indica que no se ha encontrado la página, es posible que el servicio EKM 3.0 no se esté ejecutando. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.

   Aparece la ventana de conexión de EKM 3.0.
2. Conéctese a EKM 3.0 mediante el nombre de usuario de EKM 3.0 Encryption Manager (**tklmadmin**) y la contraseña de EKM 3.0 Encryption Manager proporcionados durante la instalación de EKM 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).

Creación de una clasificación de claves maestra

En este capítulo se describe cómo crear la clasificación de claves maestra. La primera vez que se conecta a EKM 3.0, deberá crear la clasificación de claves maestra.

NOTA: Si ha migrado una clasificación de claves EKM 2.X durante la instalación de EKM 3.0, ya se habrá creado una clasificación de claves y este procedimiento no se aplica.

NOTA: Más adelante, si desea crear claves o grupos de claves adicionales, consulte Creación de grupos de claves para el grupo de dispositivos.

Para crear la clasificación de claves maestra, realice los pasos siguientes.

1. En la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager) haga clic en **Click here to create the master keystore** (Haga clic aquí para crear la clasificación de claves maestra).
   Aparecerá la pantalla **Keystore** (Clasificación de claves).
2. Conserve los valores predeterminados para los valores **Keystore type** (Tipo de clasificación de claves), **Keystore path** (Ruta de acceso a la clasificación de claves) y **Keystore name** (Nombre de la clasificación de claves).
   Los valores predeterminados son: **Keystore type** (Tipo de clasificación de claves): JCEKS y **Keystore name** (Nombre de la clasificación de claves): defaultKeyStore. El valor predeterminado de **Keystore path** (Ruta de acceso a la clasificación de claves) en Windows es: **<*root*>:\Dell\EKM\products\tklm\keystore**. El valor predeterminado para **Keystore path** (Ruta de acceso a la clasificación de claves) en Linux es: **/opt/dell/ekm/products/tklm/keystore**.
3. En el campo **Password** (Contraseña) cree una contraseña para la clasificación de claves predeterminada. Esta no debe tener menos de seis caracteres.
4. En el campo **Retype Password** (Volver a introducir contraseña), vuelva a introducir la contraseña.
5. Haga clic en **OK** (Aceptar).
   La pantalla **Keystore** (Clasificación de claves) confirma que la clasificación de claves se ha creado correctamente.
6. Cree una copia de seguridad de la clasificación de claves. Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad.

Activación del servidor de seguridad en el servidor EKM 3.0

NOTA: Consulte la documentación del sistema operativo para obtener instrucciones sobre cómo configurar el servidor de seguridad.

EKM 3.0 se comunica con la biblioteca de cintas a través de la red. Si el servidor de seguridad está activado en el sistema en el que está instalado EKM 3.0 y los puertos necesarios no se han abierto, la comunicación entre EKM 3.0 y la biblioteca de citas fallará. Si debe activar el servidor de seguridad en el sistema en el que está instalado EKM 3.0, realice los pasos siguientes para activar la comunicación entre EKM 3.0 y la biblioteca de cintas:

NOTA: Estos son todos los puertos predeterminados que usa EKM 3.0. Si la biblioteca de cintas está configurada para usar puertos diferentes, asegúrese de usar dichos números de puerto en la configuración del servidor de seguridad y en la configuración de EKM 3.0.

NOTA: Si utiliza una configuración de servidor principal/secundario para EKM 3.0, repita este procedimiento para el servidor secundario.

1. Abra los puertos siguientes para los protocolos correspondientes:
   - TCP: 3801

– SSL: 443

2. Si el servidor de seguridad está configurado para permitir solo direcciones IP o máscaras de subred específicas para la comunicación con los puertos anteriores, asegúrese de que la dirección IP o la máscara de subred de la biblioteca de cintas se incluyan en la lista de elementos permitidos.

   Para obtener acceso a la configuración de red de la biblioteca de cintas, inicie sesión en la unidad de administración remota (RMU) de la biblioteca de cintas y busque la configuración de red. Para obtener información sobre cómo buscar la guía del usuario de la biblioteca de cintas, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** del soporte de instalación de EKM 3.0.

3. Si más adelante desea cambiar la configuración de puertos para la comunicación entre EKM 3.0 y la biblioteca de cintas, asegúrese de que los puertos se cambien dentro de la configuración de la biblioteca, en EKM 3.0 y en el servidor de seguridad del sistema en el que está instalado EKM 3.0.

Configuración de EKM 3.0 para aceptar dispositivos que contactan a EKM 3.0 para obtener claves

En este capítulo se describe cómo configurar el comportamiento de EKM 3.0 para controlar dispositivos que intenten conectarse a EKM 3.0 para solicitar claves. Consulte la guía del usuario del dispositivo para obtener información sobre cómo conectarse a EKM 3.0 para solicitudes de clave.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).

2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado)** → **Key and Device Management** (Administración de claves y dispositivos).

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).

3. En el menú desplegable **Manage keys and devices** (Administrar claves y dispositivos), seleccione **LTO** y haga clic en **Go** (Ir).

NOTA: Consulte la documentación de TKLM para obtener información acerca de estos valores de configuración. Para obtener información sobre cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

4. En el menú desplegable de la parte inferior de la tabla, seleccione una de las opciones siguientes:

Automatically accept all new device requests for communication (Aceptar automáticamente todas las nuevas solicitudes de dispositivo para la comunicación)	Las claves se emitirán automáticamente a los dispositivos nuevos. Esta es la opción predeterminada para EKM 3.0. Dell recomienda conservar esta opción para el servidor principal de EKM 3.0 pero no el secundario, si hay uno configurado.
Only accept manually added devices for communication (Aceptar solamente dispositivos agregados manualmente para la comunicación)	Las claves no se emitirán a los dispositivos, a menos que se estos últimos se agreguen manualmente. Si está configurando el servidor secundario de EKM 3.0, Dell recomienda utilizar esta configuración de modo que el servidor secundario de EKM 3.0 no conceda automáticamente claves a dispositivos nuevos.
Hold new device requests pending my approval (Retener nuevas solicitudes de dispositivos pendientes de mi aprobación)	Los dispositivos que se pongan en contacto con EKM 3.0 se agregarán a una lista pendiente.

Creación de un grupo de dispositivos

Este procedimiento crea un grupo de dispositivos. Si utiliza un grupo de dispositivos predeterminado, omita esta sección.

Los grupos de dispositivos se utilizan para administrar las claves que se emiten a uno o más dispositivos. Dell recomienda que utilice grupos de dispositivos para administrar un subconjunto de dispositivos según las necesidades de la organización.

Para crear un nuevo grupo de dispositivos, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado)** → **Advanced Configuration (Configuración avanzada)** → **Device Group (Grupo de dispositivos)**.

   Aparecerá la pantalla **Manage Device Groups** (Administrar grupos de dispositivos).
3. Haga clic en **Create** (Crear) en la parte superior de la tabla.

   Aparecerá la subventana **Create Device Group** (Crear grupo de dispositivos).
4. En **Device family** (Familia de dispositivos), seleccione el botón de radio **LTO**.
5. En el campo **Device group name** (Nombre del grupo de dispositivos), introduzca un nombre de grupo de dispositivos. Dell recomienda que introduzca un nombre que refleje el uso de este grupo de dispositivos, por ejemplo, **Accounting** (Contabilidad).
6. Haga clic en **Create** (Crear).

   Una pantalla emergente **Information** (Información) indica la configuración de la familia de dispositivos.
7. En la ventana emergente **Information** (Información), haga clic en **OK** (Aceptar).

   Se creará el grupo de dispositivos. Aparecerá el nuevo grupo de dispositivos en la lista de la pantalla **Manage Device Groups** (Administrar grupos de dispositivos).

Creación de grupos de clave para un grupo de dispositivos

Los grupos de claves son para un dispositivo específico. En este capítulo se describe cómo crear y configurar grupos de claves para un dispositivo concreto. Los grupos de dispositivos configurados para un dispositivo no se pueden utilizar con otro dispositivo.

Para crear grupos de claves para un grupo de dispositivos, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado)** → **Key and Device Management (Administración de claves y dispositivos)**.

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
3. En el menú **Manage keys and devices** (Administrar claves y dispositivos), seleccione el nombre del grupo de dispositivos que desee agregar al grupo de claves.
4. Junto a **Key and Device Management** (Administración de claves y dispositivos), haga clic en **Go** (Ir).

   En la utilidad **Key and Device Management** (Administración de claves y dispositivos), se muestra una página para el grupo de dispositivos que haya seleccionado. En ella se indican los grupos de claves y los dispositivos que pertenecen a dicho grupo de dispositivos.
5. En la tabla, haga clic en **Add** (Agregar) y seleccione **Key Group** (Grupo de claves).

   Aparecerá la subventana **Create Key Group** (Crear grupo de claves).

6. En el campo **Key group name** (Nombre del grupo de claves), introduzca el nombre del grupo de claves.
7. En el campo **Number of keys to create** (Número de claves para crear), introduzca el número de claves que se deben crear.
8. En el campo **First three letters of key name** (Primeros tres letras del nombre de clave), introduzca un prefijo de tres letras para el nombre de clave.
9. Si desea que este grupo de claves sea el grupo predeterminado, seleccione la casilla **Make this the default key group** (Convertir este grupo de claves en el predeterminado).
10. Haga clic en **Create Key Group** (Crear grupo de claves).

    Aparecerá una ventana emergente **Warning** (Advertencia).
11. Si desea crear una copia de seguridad, haga clic en el vínculo azul de la ventana emergente **Warning** (Advertencia) para ir a la pantalla **Backup and Restore** (Copia de seguridad y restauración). Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad. Tras crear una copia de seguridad, vuelva a la pantalla **Key and Device Management** (Administración de claves y dispositivos). Si no desea crear una copia de seguridad en este momento, siga con el paso siguiente.

NOTA: Dell recomienda crear una copia de seguridad cuando realice cambios a claves, grupos de claves o grupos de dispositivos.

12. Haga clic en **OK** (Aceptar) en la pantalla emergente **Warning** (Advertencia).

    Se creará el grupo de claves. La pantalla **Key and Device Management** (Administración de claves y dispositivos) muestra los grupos de claves.
13. Este paso es opcional. Compruebe que las claves se han creado al realizar los pasos siguientes en la pantalla **Key and Device Management** (Administración de claves y dispositivos):
    a) En el menú desplegable de la parte superior de la tabla, seleccione **View Keys, Key Group Membership and Drives** (Ver claves, asociación a grupos de claves y unidades).

       Las claves se muestran en la tabla.
    b) Desplácese hacia abajo para buscar las claves nuevas.

Adición de un dispositivo a un grupo de dispositivos

En este capítulo se describe cómo agregar un dispositivo a un grupo de dispositivos existente.

NOTA: Los grupos de dispositivos predeterminados en EKM 3.0 son **FUTURE_DEVICES** y **LTO**.

NOTA: Para agregar un dispositivo a un grupo de dispositivos automáticamente, deberá crear un grupo clave y una copia de seguridad. De lo contrario, los diagnósticos de ruta clave de la biblioteca de cinta fallará y el dispositivo no se agregará. Consulte Creación de grupos de claves para un grupo de dispositivos y Creación de una copia de seguridad de la clasificación de claves para obtener más información.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el menú **Manage keys and devices** (Administrar claves y dispositivos) de **Key and Device Management** (Administración de claves y dispositivos) seleccione el grupo de dispositivos que desee utilizar.
3. Haga clic en **Go** (Ir).

   En la utilidad **Key and Device Management** (Administración de claves y dispositivos), se muestra una página para el grupo de dispositivos que haya seleccionado. En ella se indican los grupos de claves y los dispositivos que pertenecen a dicho grupo de dispositivos.
4. En el menú desplegable de la parte inferior de la página, seleccione, **Automatically accept all new device requests for communication** (Aceptar automáticamente todas las nuevas solicitudes de dispositivo para la comunicación).
5. Configure la biblioteca de cintas para conectarse al servidor de EKM 3.0.

Consulte la guía del usuario de la biblioteca de cintas para obtener más información. Para obtener información sobre cómo buscar la guía del usuario de la biblioteca de cintas, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

6. Ejecute los diagnósticos de ruta de clave en la unidad de administración remota (RMU) de la biblioteca de cintas. Consulte la guía del usuario de la biblioteca de cintas para obtener más información.

   El nuevo dispositivo se muestra en la pantalla **Key and Device Management** (Administración de claves y dispositivos).

NOTA: Si desea agregar un dispositivo manualmente, consulte la documentación de TKLM. Para obtener información acerca de cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Adición y eliminación de claves en los grupos de claves

En este capítulo se describe cómo agregar y eliminar claves en los grupos de claves.

NOTA: La eliminación de una clave de un grupo de claves no elimina la clave, sino que la quita del grupo de claves. Si desea eliminar una clave única, consulte Eliminación de una clave específica.

NOTA: Para obtener instrucciones sobre cómo obtener acceso a la pantalla **Key and Device Management** (Administración de claves y dispositivos), consulte Creación de grupos de claves para el grupo de dispositivos.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Key and Device Management (Administración de claves y dispositivos)**.

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
3. En el menú **Manage keys and devices** (Administrar claves y dispositivos), seleccione el nombre del grupo de dispositivos que desee agregar al grupo de claves.
4. Junto a **Key and Device Management** (Administración de claves y dispositivos), haga clic en **Go** (Ir).

   En la utilidad **Key and Device Management** (Administración de claves y dispositivos), se muestra una página para el grupo de dispositivos que haya seleccionado. En ella se indican los grupos de claves y los dispositivos que pertenecen a dicho grupo de dispositivos.
5. Seleccione el grupo de claves que desea modificar.
6. Haga clic en **Modify** (Modificar) en la parte superior de la tabla.

   Aparece la ventana secundaria **Modify Key Group** (Modificar grupo de claves).
7. En la ventana secundaria **Modify Key Group** (Modificar grupo de claves), seleccione el botón de radio deseado.

   Si selecciona el botón de radio **Create additional keys in key group** (Crear claves adicionales en el grupo de claves), introduzca el número de claves que desee agregar al grupo de claves en el campo **Number of keys to create** (Número de claves para crear). En el campo **First three letters of key name** (Tres primeras letras del nombre de clave), introduzca tres letras, que serán el prefijo de las claves nuevas.

   Si selecciona el campo **Delete key from key group** (Eliminar clave del grupo de claves), introduzca el alias de clave en el campo de texto.
8. Seleccione **Modify Key Group** (Modificar grupo de claves).

   El grupo de claves se modifica para reflejar los cambios.

Eliminación de grupos de claves

En este capítulo se describe cómo eliminar un grupo de claves.

PRECAUCIÓN: La eliminación de un grupo de claves elimina todas las claves de dicho grupo. La eliminación de una clave es igual a la eliminación de cualquier tipo de datos protegido por dicha clave, ya que los datos dejarán de estar disponibles. Por motivos de seguridad, las claves eliminadas no se pueden recuperar de ningún modo.

NOTA: No es posible eliminar el grupo de claves predeterminado de un grupo de dispositivos.

Para eliminar un grupo de claves, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.
   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Key and Device Management (Administración de claves y dispositivos)**.
   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
3. En el menú **Manage keys and devices** (Administrar claves y dispositivos), seleccione el nombre del grupo de dispositivos que desee agregar al grupo de claves.
4. Junto a **Key and Device Management** (Administración de claves y dispositivos), haga clic en **Go** (Ir).
   En la utilidad **Key and Device Management** (Administración de claves y dispositivos), se muestra una página para el grupo de dispositivos que haya seleccionado. En ella se indican los grupos de claves y los dispositivos que pertenecen a dicho grupo de dispositivos.
5. Verifique que el grupo de claves que desea eliminar no es el grupo de claves predeterminado. En dicho caso, modifique el grupo de claves de modo que no sea el predeterminado:
   a) En la tabla **Key Group** (Grupo de claves), haga clic con el botón derecho del mouse en el grupo que desee eliminar.
      Aparece un menú emergente.
   b) En él, seleccione **Modify** (Modificar).
      Aparece la ventana secundaria **Modify Key Group** (Modificar grupo de claves).
   c) Desactive la casilla **Make this the default key group** (Convertir este grupo de claves en el predeterminado).
   d) Haga clic en **Modify Key Group** (Modificar grupo de claves).
      Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
6. Seleccione el grupo de claves que desee eliminar para seleccionarlo, y haga clic en **Delete** (Eliminar).
   Aparecerá una ventana emergente de confirmación.
7. Haga clic en **OK** (Aceptar) en ella.
   Se eliminarán el grupo de claves y todas las claves asociadas al mismo.

Verificación del certificado de servidor

En este capítulo se describe cómo verificar que el certificado de servidor que desee utilizar es el certificado en uso. Para ello, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.
   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Advanced Configuration (Configuración avanzada) → Server Certificates (Certificados de servidor)**.
   Aparece la pantalla **Administer Server Certificates** (Administrar certificados de servidor).
3. Confirme que haya una marca de verificación en la columna **In Use** (en uso) del certificado que desee utilizar.
   *Si la columna **In Use** (En uso) del certificado deseado tiene una marca de verificación,* este procedimiento se habrá completado.

Si la columna ***In Use*** *(En uso) del certificado que desee utilizar no tiene una marca de verificación,* realice los pasos siguientes:

a) Haga clic en el certificado que desee utilizar para resaltarlo.
b) Haga clic en **Modify** (Modificar) en la parte superior de la tabla.
   Aparece la subventana **Modify SSL/KMIP** (Modificar SSL/KMIP).
c) Seleccione la casilla **Current certificate in use** (Certificado actual en uso).
d) Haga clic en **Modify Certificate** (Modificar certificado).
   Aparecerá una ventana emergente **Warning** (Advertencia).
e) Haga clic en **OK** (Aceptar) en la pantalla emergente **Warning** (Advertencia).
f) Detenga y reinicie el servidor. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.

NOTA: Un certificado no se puede modificar, excepto para establecerlo como **In Use** (En uso).

Visualización de los detalles del certificado de servidor

Si desea ver los detalles de certificado, realice los pasos siguientes:

1. Haga clic en el certificado para resaltarlo.
2. Haga clic en **Modify** (Modificar) en la parte superior de la tabla.
   Aparece la subventana **Modify SSL/KMIP Certificate** (Modificar certificado SSL/KMIP).
3. Visualice los detalles de certificado. También puede hacer clic en **Optional Certificate Parameters** (Parámetros de certificado opcionales) para ver los parámetros opcionales.

Conexión al servidor WebSphere

Algunos procedimientos que se describen en esta guía requieren la conexión al servidor WebSphere. En este capítulo se describe cómo conectarse el servidor WebSphere en Windows y Linux. Solo es necesario conectarse al servidor WebSphere si así lo indica en otro procedimiento.

Para conectarse al servidor WebSphere mediante el comando **wsadmin**:

1. *En Windows,* en un símbolo del sistema, vaya a **<*root*>:\Dell\EKM\bin**. *En Linux,* en una sesión de terminal, vaya a **/opt/dell/ekm/bin**.
2. *Para Windows,* introduzca el comando siguiente:
   ```
   wsadmin -username tklmadmin -password <tklm password> -lang jython
   ```
   Para Linux, introduzca el comando siguiente:
   ```
   ./wsadmin.sh -username tklmadmin -password <tklm password> -lang jython
   ```
   Presione **Intro**. El comando se ejecuta durante un tiempo breve y aparecerá el símbolo del sistema **wsadmin**.

NOTA: Los comandos distinguen entre minúsculas y mayúsculas. No se deben colocar espacios entorno a los paréntesis o corchetes. No introduzca símbolos de menor que y mayor que (< >) alrededor de las variables.

NOTA: Para desconectarse del WebSphere, escriba **Exit** y presione **Intro**.

Inicio y detención del servidor EKM 3.0 en Windows

En este capítulo se describe como iniciar y detener el servidor EKM 3.0 en Windows.

1. En un símbolo del sistema, vaya a **<*root*>:\Dell\EKM\bin**.
2. Para iniciar el servidor, introduzca el comando siguiente:

   ```
   startserver server1
   ```

   Para detener el servidor, introduzca el comando siguiente:

   ```
   stopserver server1
   ```
3. Presione **Intro**.

   El comando se ejecuta y el símbolo del sistema muestra el mensaje de confirmación:

   ```
   Server server1 open for e-business (El servidor server1 está listo para
   comercio electrónico)
   ```

   O bien

   ```
   Server server1 stop completed (Se ha completado la detención del servidor
   server1)
   ```

Inicio y detención del servidor EKM 3.0 en Linux

En este capítulo se describe como iniciar y detener el servidor EKM 3.0 en Linux.

NOTA: Debe conectarse como usuario raíz para iniciar y detener el servidor.

1. En una sesión de terminal, vaya a **/opt/dell/ekm/bin**.
2. Para iniciar el servidor, introduzca el comando siguiente:

   ```
   ./startserver.sh server1
   ```

   Para detener el servidor, introduzca el comando siguiente:

   ```
   ./stopserver.sh server1
   ```

NOTA: Se le solicitará el administrador y la contraseña de EKM 3.0 para poder detener el servidor.

3. Presione **Intro**.

   El comando se ejecuta y la sesión de terminal muestra el mensaje de confirmación:

   ```
   Server server1 open for e-business (El servidor server1 está listo para
   comercio electrónico)
   ```

   O bien

   ```
   Server server1 stop completed (Se ha completado la detención del servidor
   server1)
   ```

6

Migración y combinación

Durante la instalación de EKM 3.0 es posible migrar EKM 2.X en EKM 3.0.

Después de la instalación de EKM 3.0 es posible combinar EKM 2.X en EKM 3.0.

En este capítulo se describen los procedimientos de combinación y migración.

NOTA: Solo es posible migrar o combinar una versión EKM 2.X que se haya utilizado para crear claves.

Migración de Encryption Key Manager (EKM) versión 2.X durante la instalación de EKM 3.0

Realice este procedimiento solamente si está configurando la pantalla **Migration** (Migración) durante la instalación de EKM 3.0. La pantalla **Migration** (Migración) se utiliza para migrar Encryption Key Manager (EKM) versión 2.X en EKM 3.0.

NOTA: Si actualmente utiliza EKM 2.X, Dell recomienda conservar la infraestructura actual (servidores, sistemas operativos, bibliotecas de cinta, etc. que están bajo la protección de EKM 2.X), a menos que esté experimentando problemas.

Si es necesario migrar EKM versión 2.X a EKM 3.0, Dell recomienda que se realice ahora.

NOTA: Si utiliza EKM 2.X con una máquina virtual como host de EKM 2.X, deberá conservar EKM 2.X o migrar a un servidor físico. EKM 3.0 no admite el uso de máquinas virtuales como hosts.

NOTA: Durante la instalación de EKM 3.0 solo es posible migrar una única instancia de EKM versión 2.X. Si dispone de más de una instancia de EKM versión 2.X que se debe conectar a EKM 3.0 mediante un puerto, migre la primera mediante este procedimiento. A continuación, una vez completada la instalación, consulte Combinación de instancias adicionales de EKM versión 2.X en EKM 3.0 para combinar versiones adicionales.

Es posible *combinar* EKM versión 2.X en EKM 3.0 una vez completada la instalación de EKM 3.0 mediante la herramienta de combinación EKM 2.X a EKM 3.0. Sin embargo, Dell recomienda que realice la migración en este momento.

NOTA: Si utiliza una configuración de servidor EKM 3.0 principal/secundario, deberá realizar el procedimiento de migración solamente en el servidor EKM 3.0 principal.

Una vez completada la migración, realice una copia de seguridad del servidor EKM 3.0 principal y utilice dicha copia para restaurar el servidor EKM 3.0 secundario de modo que coincida con el servidor EKM 3.0 principal.

Para migrar desde EKM 2.X durante el proceso de instalación de EKM 3.0, diríjase a Procedimiento de migración de EKM 2.X a EKM 3.0.

Procedimiento de migración de EKM 2.X a EKM 3.0

Para migrar la versión de EKM 2.X a EKM 3.0 desde la pantalla **Migration** (Migración) durante la instalación de EKM 3.0, realice los pasos siguientes:

1. Conéctese a la consola de EKM 2.X, cree una copia de seguridad de la clasificación de claves de EKM 2.X, detenga el servidor de EKM 2.X y salga de la consola de EKM 2.X. Consulte la guía del usuario de EKM 2.X para obtener más información.
2. Copie la carpeta EKM 2.X:

   Si el servidor de EKM 2.X está instalado en un equipo distinto que el equipo de instalación de EKM 3.0, copie la carpeta de EKM 2.X del servidor de EKM 2.X a una carpeta temporal del servidor EKM 3.0 (por ejemplo, **C:\temp \MyEKM2** en Windows o **/opt/myekm2** en Linux).

   Si el servidor EKM 2.X está instalado en el mismo equipo que el equipo de instalación de EKM 3.0 de destino, aún deberá crear una copia de la carpeta de EKM 2.X en ese equipo.
3. En la pantalla **Migration** (Migración) de la instalación de EKM 3.0, active la casilla **Migrate from EKM 2.X to EKM 3.0** (Migrar de EKM 2.X a EKM 3.0).
4. Haga clic en **Choose** (Elegir) y vaya al directorio en el que ha copiado la carpeta EKM 2.X. No seleccione ningún elemento de esta carpeta.

PRECAUCIÓN: Si el servidor de EKM 2.X está instalado en el mismo equipo que el equipo de instalación del EKM 3.0 de destino, no vaya al directorio en el que está instalado EKM 2.X, ya que el instalador EKM 3.0 elimina la carpeta que se utiliza para la migración. Vaya a la copia del directorio de EKM 2.X que ha creado.

5. Haga clic en **Next** (Siguiente).
   Aparece la pantalla **Configuration Summary** (Resumen de la configuración).

NOTA: Si aparece un mensaje de error, verifique la ruta de acceso al directorio de EKM 2.X.

6. Siga con la instalación de EKM 3.0. Consulte Proceda a Procedimiento de instalación de EKM 3.0.

NOTA: La contraseña para la nueva clasificación de claves EKM 3.0 es la misma contraseña asociada con la clasificación de claves de EKM 2.X que se utiliza para la migración.

PRECAUCIÓN: No ejecute EKM 2.X después de haber migrado sus claves a EKM 3.0. Si desea, puede desinstalar EKM 2.X después de migrar correctamente de EKM 2.X a EKM 3.0. Dell recomienda que realice una copia de seguridad de los archivos de EKM 2.X antes de desinstalar EKM 2.X.

Combinación de Encryption Key Manager (EKM) 2.X en EKM 3.0 después de instalar EKM 3.0

En este capítulo se describe el procedimiento de combinación de EKM 2.X en EKM 3.0 después de instalación para Windows y Linux. Este procedimiento utiliza la herramienta de combinación EKM 2.X a EKM 3.0.

Utilice este procedimiento si EKM 3.0 ya está instalado y configurado, y desea combinar EKM 2.X en EKM 3.0.

NOTA: Si utiliza una configuración de servidor EKM 3.0 principal/secundario, deberá realizar el procedimiento de combinación solamente en el servidor EKM 3.0 principal. Una vez completado el procedimiento de combinación en el servidor EKM 3.0 principal, realice el procedimiento de creación de copia de seguridad y, a continuación, restaure el archivo de copia de seguridad en el servidor EKM 3.0 secundario. Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad.

NOTA: Si EKM 3.0 todavía no está instalado, Dell recomienda migrar EKM 2.X en EKM 3.0 durante la instalación de EKM 3.0. Consulte Procedimiento de instalación de EKM 3.0.

En los ejemplos de este documento se utilizan las rutas de acceso estándares de Windows (por ejemplo, **C:\<*foldername*>**). Sustituya la letra de la unidad raíz o la ruta de acceso Linux adecuada para el sistema.

Requisitos previos de la herramienta de combinación

Antes de ejecutar la herramienta de combinación, compruebe que se han cumplido los requisitos siguientes:

- EKM 3.0 debe estar instalado y se debe haber creado la clasificación de claves maestra. De lo contrario, fallará el procedimiento de combinación. Consulte Creación de una clasificación de claves maestra.
- Al realizar una combinación de EKM 2.X a EKM 3.0, EKM 2.X y EKM 3.0 deben estar instalados en la misma versión de sistema operativo.
- Si ha combinado o migrado anteriormente EKM 2.X en EKM 3.0, el certificado **ekmcert** de la combinación o migración anterior aún existirá en el servidor de EKM 3.0 y puede existir incluso se ha realizado una restauración de una copia de seguridad anterior. Deberá quitar el certificado **ekmcert** del servidor de EKM 3.0 antes de realizar el procedimiento de combinación. Consulte Eliminación del certificado ekmcert, claves y grupos de claves, y cambio de nombre de los dispositivos.
- Debe cambiar el nombre de las claves, los grupos de claves y los dispositivos duplicados en EKM 2.X antes de combinarlos en EKM 3.0. Consulte la guía de usuario de EKM 2.X.
  - No puede haber alias/nombres de clave duplicados desde el origen de EKM 2.X con el EKM 3.0 de destino. Cada clave entrante debe tener un alias/nombre único. De lo contrario, fallará el procedimiento de combinación.
  - No puede haber alias/nombres de *grupos* de clave duplicados desde el origen de EKM 2.X con el EKM 3.0 de destino. Cada clave entrante debe tener un alias/nombre único. De lo contrario, fallará el procedimiento de combinación.
  - No puede haber dispositivos duplicados desde el origen de EKM 2.X con el EKM 3.0 de destino. De lo contrario, fallará el procedimiento de combinación.

Procedimiento de combinación de EKM 2.X a EKM 3.0

Realice los pasos siguientes para ejecutar la herramienta de combinación:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el servidor de EKM 3.0, cree una copia de seguridad de EKM 3.0. Consulte Creación de copias de seguridad y restauración a partir de una copia de seguridad para conocer el procedimiento de creación de copias de seguridad.

   Si falla la herramienta de combinación o esta daña los datos de EKM 3.0, puede utilizar las copias de seguridad para recuperar la información perdida.
3. Desconéctese de EKM 3.0.
4. Detenga el servidor de EKM 3.0 antes de ejecutar la herramienta de combinación. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.
5. En la raíz del servidor de EKM 3.0, cree una carpeta adecuada (por ejemplo, **C:\EKM_Files** en Windows o **/opt/EKM_Files** en Linux).
6. Conéctese a la consola de EKM 2.X, cree una copia de seguridad de la clasificación de claves de EKM 2.X, detenga el servidor de EKM 2.X y salga de la consola de EKM 2.X. Consulte la guía del usuario de EKM 2.X.
7. En la ubicación en la que está instalado EKM 2.X, copie los archivos siguientes a la carpeta creada en el servidor de EKM 3.0 durante el paso anterior. Si EKM 2.X está instalado en un sistema físico diferente, utilice una unidad extraíble o un recurso compartido de servidor con el mismo sistema operativo.
   - En Windows, desde **<*root*>:\ekm\gui**, copie **EKMKeys.jck**. En Linux, la ubicación es **/var/ekm/gui**.
   - En Windows, desde **<*root*>:\ekm\gui**, copie el archivo **KeyManagerConfig.properties** (el archivo de configuración de EKM). En Linux, la ubicación es **/var/ekm/gui**.

- En Windows, desde **<*root*>:\ekm\gui\keygroups**, copie el archivo **keygroup.xml**. En Linux, la ubicación es **/var/ekm/gui/keygroups**.
- En Windows, desde **<*root*>:\ekm\gui\drivetable**, copie el archivo **ekm_drivetable.dt**. En Linux, la ubicación es **/var/ekm/gui/drivetable**.

PRECAUCIÓN: En Windows, utilice el Bloc de Notas para crear o editar los archivos de texto. Si utiliza Wordpad, el procedimiento fallará.

8. Edite el archivo **KeyManagerConfig.properties** de modo que contenga solo las propiedades siguientes:
   - **config.keygroup.xml.file**
   - **config.keystore.password.obfuscated**
   - **config.keystore.file**
   - **config.drivetable.file.url**

   Elimine las demás líneas. Para obtener un ejemplo, consulte la sección Ejemplo de código de este procedimiento.
9. Agregue las siguientes opciones de DB2 al nuevo archivo **KeyManagerConfig.properties**:
   - jdbcURL = jdbc:db2://localhost:<*EKM 3.0 DB2 database port*>/<*EKM 3.0 DB2 database name*>

     O bien

     jdbcURL = jdbc:db2://<*dEKM 3.0 server IP address*>:<*EKM 3.0 DB2 database port*>/<*EKM 3.0 DB2 database name*>
   - jdbcUID = <*DB2 administrator user name*>
   - jdbcPW = <*DB2 administrator password*>
   - dbType = DB2

   Para obtener un ejemplo, consulte la sección Ejemplo de código de este procedimiento.

NOTA: Las variables son parámetros que establece al instalar EKM 3.0. No introduzca los símbolos de menor que y mayor que (< >) alrededor de las variables. Las variables, los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas.

10. Agregue la entrada de contraseña para la clasificación de claves predeterminada de EKM 3.0 al archivo **KeyManagerConfig.properties**. La entrada de contraseña es:

    tklm.encryption.password = <*ekm 3.0 keystore password*>.

    El archivo **KeyManagerConfig.properties** actualizado debería tener un aspecto parecido al ejemplo siguiente:

Ejemplo de código para Windows

```
config.keygroup.xml.file = File:c:\\<EKM_Files>\\KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = c:\\<EKM_Files>\\EKMKeys.jck
config.drivetable.file.url = File:c:\\<EKM_Files>\
\ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/
ekm_dell jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Donde *EKM_Files* es la carpeta creada anteriormente.

Ejemplo de código para Linux

```
config.keygroup.xml.file = File:/opt/<EKM_Files>/KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = /opt/<EKM_Files>/EKMKeys.jck
config.drivetable.file.url = File:/opt/<EKM_Files>/
ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Donde *EKM_Files* es la carpeta creada anteriormente.

11. Vaya a la carpeta **EKM2DKMMerge** del soporte de instalación de EKM 3.0. Desde la carpeta **EKM2DKMMerge**, copie el archivo **EKM2DKMMerge.jar** a la carpeta creada anteriormente en este procedimiento (por ejemplo C:\EKM_Files en Windows u /opt/EKM_Files en Linux).

NOTA: Debe utilizar el mismo símbolo del sistema o sesión de terminal para realizar todos los pasos subsiguientes. Si cambia los símbolos del sistema o las sesiones de terminal, el valor de CLASSPATH que establezca no se aplicará automáticamente a los demás símbolos del sistema o sesiones de terminal.

12. En el servidor de EKM 3.0, configure las rutas de acceso para WAS y TIP que necesitará la herramienta de combinación.

En Windows:

a. En un símbolo del sistema, vaya a **<*root*>:\Dell\EKM\bin**.

b. Introduzca el comando siguiente para ejecutar la secuencia de comandos del símbolo del sistema:

```
setupCmdLine.bat
```

Ejemplo:

```
C:\Dell\EKM\bin\setupCmdLine.bat
```

c. Presione **Intro**. El comando se ejecuta y el sistema muestra el texto siguiente en la última línea:

```
goto :EOF
```

En Linux:

a. En una sesión de terminal, vaya a **/opt/dell/ekm/bin**.

b. Introduzca el comando siguiente:

```
. setupCmdLine.sh
```

c. Se ejecuta el comando. Una vez que el comando se haya completado correctamente en Linux, aparecerá un símbolo del sistema en blanco. No hay ningún indicador de que el comando se ha completado.

NOTA: La secuencia de comandos **setupCmdLine.sh** debe disponer de permisos de ejecución.

13. Cree un archivo de lote de línea de comandos (.bat) (en Linux, .sh) para insertar los archivos .jar que necesita la herramienta de combinación y para establecer parámetros adicionales de CLASSPATH:

a) Copie la siguiente configuración temporal de CLASSPATH en un archivo de texto y asígnele el nombre <*filename*>.bat o en Linux, <*filename*>.sh (por ejemplo, **setupclasspath.bat** en Windows o **setupclasspath.sh** en Linux).

b) Guarde el archivo.bat/.sh en la carpeta creada durante este procedimiento. Por ejemplo, C:\EKM_Files u /opt/EKM_Files.

PRECAUCIÓN: En Windows, utilice el Bloc de Notas para crear o editar los archivos de texto. Si utiliza Wordpad, el procedimiento fallará.

c) Edite el archivo de lote:

En Windows, edite el archivo de lote para reemplazar ***c:\EKM\Needed*** con la ruta en la que ha colocado el archivo **EKM2DKMMerge.jar**. Por ejemplo, **c:\EKM_Files**.

En Linux, edite la secuencia de comandos de la shell para reemplazar **/opt/EKM_Files** con la ruta en la que ha colocado el archivo **EKM2DKMMerge.jar**.

Configuración temporal de CLASSPATH para Windows

```
set JAVA_HOME=%WAS_HOME%\java set PATH=%JAVA_HOME%\bin;%JAVA_HOME%\jre
\bin;%PATH% set CLASSPATH=c:\EKM\Needed\EKM2DKMMerge.jar;%CLASSPATH% set
CLASSPATH=.;%WAS_HOME%\plugins\com.ibm.icu_3.4.5.jar;%WAS_HOME%\products
\tklm\migration\j2ee.jar;%WAS_HOME%\plugins\com.ibm.tklm.commands.jar;
%WAS_HOME%\products\tklm\migration\com.ibm.tklm.kmip.adapter.jar;%WAS_HOME
%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.kmip.jar;"C:\Archivos de programa\Dell\db2dkm\java
\db2jcc.jar";"C:\Archivos de programa\Dell\db2dkm\java
\db2jcc_license_cu.jar";%WAS_HOME%\profiles\TIPProfile\installedApps
```

```
\TIPCell\tklm_kms.ear\com.ibm.tklm.keyserver.jar;%WAS_HOME%\profiles
\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.server.api.jar;%WAS_HOME%\profiles\TIPProfile\installedApps
\TIPCell\tklm_kms.ear\com.ibm.tklm.server.db.ejb.jar;%CLASSPATH%
```

NOTA: Reemplace las letras de unidad según sea necesario.

NOTA: Si utiliza Windows de 64 bits, edite el archivo de lote para reemplazar **Archivos de programa** en el valor de CLASSPATH anterior con **Archivos de programa (x86)**.

Configuración temporal de CLASSPATH para Linux

```
export JAVA_HOME=$WAS_HOME/java export PATH=${JAVA_HOME}/bin:${JAVA_HOME}
$/jre/bin:$PATH export CLASSPATH=/opt/EKM_Files/EKM2DKMMerge.jar:
$CLASSPATH export CLASSPATH=.:$WAS_HOME/plugins/com.ibm.icu_3.4.5.jar:
$WAS_HOME/products/tklm/migration/j2ee.jar:$WAS_HOME/plugins/
com.ibm.tklm.commands.jar:$WAS_HOME/products/tklm/migration/
com.ibm.tklm.kmip.adapter.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.kmip.jar:/opt/dell/db2ekm/java/
db2jcc.jar:/opt/dell/db2ekm/java/db2jcc_license_cu.jar:$WAS_HOME/profiles/
TIPProfile/installedApps/TIPCell/tklm_kms.ear/com.ibm.tklm.keyserver.jar:
$WAS_HOME/profiles/TIPProfile/installedApps/TIPCell/tklm_kms.ear/
com.ibm.tklm.server.api.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.server.db.ejb.jar:$CLASSPATH
```

14. Ejecute el archivo de lote recién creado. En el mismo símbolo del sistema o sesión de terminal en el servidor EKM 3.0, vaya a la carpeta creada anteriormente durante este procedimiento (por ejemplo, C:\EKM_Files en Windows u /opt/EKM_Files en Linux) y ejecute el archivo de lote creado en el paso anterior. En Linux, inserte el archivo creado anteriormente, por ejemplo, . setupclasspath.sh.

15. En el mismo símbolo del sistema o sesión de terminal en el servidor EKM 3.0, ejecute el comando Java siguiente:

```
java<space>com.ibm.tklm.ekm2tklm.MergeEKM2KLM<space>KeyManagerConfig.propert
ies
```

NOTA: Los comandos distinguen entre mayúsculas y minúsculas. No introduzca símbolos de menor que y mayor que (< >) alrededor de las variables.

El archivo **KeyManagerConfig.properties** es el archivo que ha actualizado anteriormente durante este procedimiento.

Este comando combina EKM 2.X con EKM 3.0.

Al completarse correctamente la operación, aparecerá el mensaje siguiente:

```
TKLM version: 2.0.0.0 201007241325Starting EKM to KLM MergeKMSDebug.init,
debug output filename not specified: using defaultCTGKS0250I: Successfully
migrated the Encryption Key Manager keystores, certificates and
keys.CTGKS0251I: Successfully migrated the Encryption Key Manager key
groups.CTGKS0249I: Successfully migrated the Encryption Key Manager
devices.Migration Complete. (TKLM versión: 2.0.0.0 201007241325 Iniciando
EKM en KLM MergeKMSDebug.init, nombre de archivo de salida de depuración no
especificado: utilizando predeterminadoCTGKS0250I: las clasificaciones de
claves, los certificados y las claves de Encryption Key Manager se han
migrado correctamente. CTGKS0251I: los grupos de claves de Encryption Key
Manager se ha migrado correctamente. CTGKS0249I: los dispositivos de
Encryption Key Manager se han migrado correctamente. Migración completada).
```

NOTA: Si recibe errores, consulte el archivo de depuración para determinar la causa. Si desea, puede guardar el archivo de depuración en otra ubicación o cambiar su nombre para que sea más estático. De lo contrario, la herramienta de combinación EKM 2.X a EKM 3.0 anexará datos al mismo. En Windows, el registro de depuración se encuentra en el directorio siguiente del servidor de EKM 3.0: **<*root*>:\Dell\EKM\bin\products\tklm\logs\debug.log**. En Linux, el registro de depuración se encuentra en el directorio siguiente del servidor de EKM 3.0: **/opt/dell/ekm/bin/products/tklm/logs/debug.log**.

NOTA: Si recibe el error siguiente, significa que intenta migrar mientras un elemento duplicado se encuentra en el servidor de EKM 2.X y el servidor de EKM 3.0:

```
Duplicate <item> = <item>Migration failed. Please refer to the debug file
for more information. (Duplicado <elemento> = <elemento>. Falló la
migración. Consulte el archivo de depuración para obtener más información).
```

Consulte Eliminación del certificado ekmcert, las claves y los grupos de claves, y cambio de nombre de los dispositivos

Si recibe el error siguiente y desea eliminar la clave en lugar de cambiar su nombre, no cierre el símbolo del sistema o la sesión de terminal. Deberá copiar el alias de clave desde el símbolo del sistema o la sesión de terminal.

```
Duplicate Key Alias= <key alias> (Alias de clave duplicado =<alias de
clave>)
```

Consulte Eliminación del certificado ekmcert, las claves y los grupos de claves, y cambio de nombre de los dispositivos

PRECAUCIÓN: La eliminación de una clave es igual a la eliminación de cualquier tipo de datos protegido por dicha clave, ya que los datos dejarán de estar disponibles. Por motivos de seguridad, las claves eliminadas no se pueden recuperar de ningún modo.

16. Inicie el servidor de EKM 3.0 mediante el comando **startserver**. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.

17. Verifique que los grupos de claves, las claves y los dispositivos de EKM 2.X hayan migrado a EKM 3.0. Consulte verificación de la combinación o migración de EKM 2.X a EKM 3.0. Si el procedimiento de combinación se ha realizado correctamente, el procedimiento se habrá completado. Si desea combinar instancias adicionales de EKM versión 2.X en EKM 3.0, consulte Combinación de instancias adicionales de EKM versión 2.X en EKM 3.0. Si el procedimiento de combinación no se ha completado correctamente, consulte Fallo de combinación.

PRECAUCIÓN: No ejecute EKM 2.X después de haber combinado sus claves en EKM 3.0. Si lo desea, puede desinstalar EKM 2.X tras combinar correctamente de EKM 2.X a EKM 3.0. Dell recomienda crear una copia de seguridad de los archivos de EKM 2.X antes de desinstalar EKM 2.X.

Verificación de la combinación o migración de EKM 2.X a EKM 3.0

En este capítulo se describe cómo verificar si los procedimientos de combinación o migración de EKM 2.X a EKM 3.0 se han realizado correctamente y si las bibliotecas de cintas son funcionales.

Para verificar que EKM 2.X se ha combinado o migrado correctamente en EKM 3.0, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).

2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Key and Device Management (Administración de claves y dispositivos)**.

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).

3. En el menú desplegable **Manage keys and devices** (Administrar claves y dispositivos), seleccione **LTO** y haga clic en **Go** (Ir).

   La pantalla **Key and Device Management** (Administración de claves y dispositivos) muestra los grupos de claves de EKM migrados y el número de claves en cada grupo.

4. En el menú desplegable de la parte superior de la tabla, seleccione **View Keys, Key Group Membership and Drives** (Ver claves, asociación de grupos de clave y unidades). Si aparecen claves en el lado izquierdo de la tabla, la combinación se ha realizado correctamente.

5. La migración no importa los dispositivos configurados de EKM 2.X. Deberá configurar los dispositivos de EKM 2.X. Consulte Adición de un dispositivo a un grupo de dispositivos.
6. En el portal de EKM 3.0, verifique que EKM 3.0 está configurado para aceptar solicitudes de dispositivos automáticamente. La opción de la pantalla **Key and Device Management** (Administración de claves y dispositivos) debería configurarse en **Automatically accept all new device requests for communication** (Aceptar automáticamente todas las solicitudes de dispositivo nuevas para la comunicación).
7. Verifique los dispositivos de la biblioteca:
   a) Verifique que los puertos SSL y TCP se han configurado correctamente en la biblioteca de cintas.
   b) Ejecute los diagnósticos de la ruta de acceso de claves desde la biblioteca de cintas para verificar la configuración de esta última.

NOTA: Consulte la guía del usuario de la biblioteca de cintas para obtener más información. Para obtener información sobre cómo buscar la guía del usuario de la biblioteca de cintas, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Fallo de combinación

Si falla el procedimiento de combinación, realice los pasos siguientes:

1. Verifique que se ha iniciado el servidor de EKM 3.0. De lo contrario, inicie el servidor de EKM 3.0 mediante el comando **startserver**. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.
2. Cierre el símbolo del sistema.
3. Para capturar el registro de depuración, guárdelo en otra ubicación o cambie su nombre.

   El registro de depuración se encuentra en el directorio siguiente: ***<root>*:\Dell\EKM\bin\products\tklm\logs\debug.log** en Windows u **/opt/dell/ekm/bin/products/tklm/logs/debug.log** en Linux.
4. Restaure EKM 3.0 a través del portal de EKM 3.0 a partir de la copia de seguridad que ha creado en el primer paso del Procedimiento de combinación de EKM 2.X a EKM 3.0. Para obtener instrucciones sobre cómo realizar una restauración a partir de una copia de seguridad, consulte Restauración desde una copia de seguridad.
5. Vuelva a realizar el procedimiento de combinación. Consulte Procedimiento de combinación de EKM 2.X a EKM 3.0.

Combinación de instancias adicionales de EKM versión 2.X en EKM 3.0

Realice este procedimiento si ha migrado o combinado EKM 2.X en EKM 3.0 y desea combinar instancias adicionales de EKM versión 2.X en EKM 3.0.

1. Quite el certificado **ekmcert** del EKM 3.0. Consulte Eliminación del certificado ekmcert, las claves y los grupos de claves y cambio de nombre de los dispositivos.
2. Realice el procedimiento siguiente para cada instancia adicional de EKM versión 2.X que desee combinar. Consulte Procedimiento de combinación de EKM 2.X a EKM 3.0.

Eliminación del certificado ekmcert, claves y grupos de claves y cambio de nombre de dispositivos

Al realizar una combinación de EKM 2.X a EKM 3.0, no puede haber certificados **ekmcert**, alias de clave, alias de grupo de claves o dispositivos duplicados en EKM 2.X ni en el servidor EKM 3.0.

NOTA: Si hay claves o grupos de claves duplicados, Dell recomienda que cambie el nombre de los mismos en EKM 2.X antes de combinarlos en EKM 3.0. Consulte la guía de usuario de EKM 2.X para obtener más información. Si las claves o los grupos de claves están obsoletos, puede eliminarlos en EKM 2.X. Sin embargo, tenga en cuenta que la eliminación de una clave equivale a la eliminación de los datos que esta protege, ya que dichos datos dejarán de estar disponibles. Por motivos de seguridad, las claves eliminadas no se pueden recuperar de ningún modo.

Si tiene dispositivos duplicados, deberá eliminar uno de ellos en EKM 2.X.

Si recibe el error siguiente al realizar el procedimiento de combinación, elimine el elemento adecuado según se indica en el mensaje.

```
Duplicate <item> = <item> Migration failed. Please refer to the debug file for
more information. (<elemento> duplicado = <elemento>. Falló la migración.
Consulte el archivo de depuración para obtener más información).
```

Consulte la sección adecuada:

- Eliminación del certificado ekmcert
- Eliminación de una clave específica
- Eliminación de un dispositivo

Eliminación del certificado ekmcert

Cada instalación de EKM 2.X tiene un certificado **ekmcert**. Si está combinando o migrando más de una instancia de EKM 2.X a EKM 3.0, deberá eliminar el certificado **ekmcert** en EKM 3.0 antes de intentar combinar a una nueva instancia de EKM 2.X.

Dado que **ekmcert** es un certificado y no una clave, no forma parte de ningún grupo de claves en el servidor de EKM 3.0. Por tanto, si ha combinado una instancia de EKM versión 2.X en EKM 3.0 y luego ha quitado grupos de claves EKM 2.X de EKM 3.0, el certificado **ekmcert** de la combinación aún existirá en el servidor de EKM 3.0 y podría existir incluso si realiza una restauración a partir de una copia de seguridad anterior. Dado que la herramienta de combinación intenta agregar nuevamente el certificado **ekmcert**, la combinación fallará.

Debe quitar el certificado **ekmcert** del servidor de EKM 3.0 si existe cualquiera de las situaciones siguientes:

- Ha migrado una instancia de EKM 2.X a EKM 3.0 durante el procedimiento de instalación de EKM 3.0.
- No se trata de la primera vez que ha combinado EKM 2.X en EKM 3.0.
- Debe eliminar una versión de EKM 2.X combinada o migrada anteriormente.
- Recibe el error siguiente al intentar una combinación. Este error indica que el certificado **ekmcert** ya se encuentra en EKM 3.0:

  ```
  Duplicate Key Alias = ekmcert Migration failed. Please refer to the debug file for more information. (Alias de clave duplicado = ekmcert. Fallo de migración. Consulte el archivo de depuración para obtener más información).
  ```

Para eliminar el certificado **ekmcert**, consulte Eliminación del certificado ekmcert.

Eliminación del certificado ekmcert

Para verificar que el certificado **ekmcert** se encuentra en EKM 3.0 y eliminarlo, realice los pasos siguientes:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado)** → **Advanced Configuration (Configuración avanzada)** → **Server Certificates (Certificados de servidor)** .

   Aparece la pantalla **Administer Server Certificates** (Administrar certificados de servidor).
3. En la pantalla **Administer Server Certificates** (Administrar certificados de servidor), verifique que el certificado **ekmcert** figura en la lista y no está en uso.

   Si el certificado **ekmcert** no se utiliza, vaya al paso siguiente. Si el certificado **ekmcert** está en uso, realice los pasos siguientes:

   a) Seleccione el certificado **ekmcert**.
   b) Haga clic en **Modify** (Modificar).
   c) Desactive la casilla **Current Certificate In Use** (Certificado actual en uso).
   d) Haga clic en **Modify Certificate** (Modificar certificado).

      Aparece la pantalla **Administer Server Certificates** (Administrar certificados de servidor). El certificado que se muestra como que no está en uso.
4. Seleccione el certificado **ekmcert** otra vez.
5. Haga clic en **Delete** (Eliminar) en la parte superior de la tabla.

   Aparece una ventana de confirmación.
6. Haga clic en **OK** (Aceptar) para eliminar el certificado.

   El certificado se quita de la lista.

Eliminación de una clave específica

En este capítulo se describe cómo eliminar una sola clave. No es posible eliminar una clave asociada a un dispositivo.

PRECAUCIÓN: La eliminación de una clave es igual a la eliminación de cualquier tipo de datos protegido por dicha clave, ya que los datos dejarán de estar disponibles. Por motivos de seguridad, las claves eliminadas no se pueden recuperar de ningún modo.

NOTA: Si ha recibido un mensaje de error que indica que tiene una clave duplicada al realizar una combinación de EKM 2.X a EKM 3.0, Dell recomienda que cambie el nombre de la clave duplicada en EKM 2.X. Consulte la guía del usuario de EKM 2.X para obtener más información.

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Key and Device Management (Administración de claves y dispositivos)**.

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
3. En el menú desplegable **Manage keys and devices** (Administrar claves y dispositivos), seleccione **LTO** y haga clic en **Go** (Ir).

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
4. En el menú desplegable de la parte superior de la tabla, seleccione **View Keys, Key Group Membership and Drives** (Ver claves, asociación a grupos de claves y unidades).

   Las claves se muestran en la tabla.
5. Haga clic en la clave que desea eliminar para seleccionarla.
6. Haga clic en **Delete** (Eliminar) en la parte superior de la tabla.

   Aparecerá una ventana emergente de confirmación.
7. Si está seguro de que desea eliminar la clave seleccionada, haga clic en **Aceptar** (Aceptar).

   Se elimina la clave.

Eliminación de un dispositivo

En este capítulo se describe cómo eliminar un dispositivo. Un dispositivo es una unidad individual instalada en la biblioteca de cintas. El número de serie se muestra en el lado derecho de la unidad de cinta.

NOTA: Si ha recibido un mensaje de error que indica que tiene un dispositivo duplicado al realizar una combinación de EKM 2.X a EKM 3.0, Dell recomienda que elimine el dispositivo en EKM 2.X. Consulte la guía del usuario de EKM 2.X para obtener más información.

Realice los pasos siguientes para eliminar el dispositivo de EKM 3.0:

1. Conéctese al portal de EKM 3.0. Consulte Conexión al portal de Encryption Key Manager 3.0.

   Aparece la pantalla **Welcome to Dell Encryption Key Manager** (Bienvenido a Dell Encryption Key Manager).
2. En el panel de navegación, vaya a **Dell Encryption Key Manager (Administrador de claves de cifrado) → Key and Device Management (Administración de claves y dispositivos)**.

   Aparece la pantalla **Key and Device Management** (Administración de claves y dispositivos).
3. En el menú **Manage keys and devices** (Administrar claves y dispositivos), seleccione el grupo de dispositivos que contiene el dispositivo que desee eliminar.
4. Haga clic en **Go** (Ir).

   Se enumeran los dispositivos que pertenecen al grupo de dispositivos.
5. Haga clic en el dispositivo que desea eliminar para seleccionarlo.
6. Haga clic en **Delete** (Eliminar) en la parte superior de la tabla.

   Aparecerá una ventana emergente de confirmación.
7. Haga clic en **OK** (Aceptar) en la pantalla emergente.

   Se elimina el dispositivo.

Verificación que la biblioteca de clasificaciones de claves de EKM 2.X se ha eliminado de EKM 3.0

Este procedimiento es opcional. En este capítulo se describe cómo verificar que todas las entradas de clasificaciones de claves de EKM 2.X (el certificado **ekmcert** y las claves de la clasificación de claves de EKM 2.X) se han quitado del servidor de EKM 3.0. Para ello, realice los pasos siguientes:

1. En un símbolo del sistema o sesión de terminal en el servidor de EKM 3.0, vaya a la carpeta creada durante el procedimiento de combinación de EKM 2.X a EKM 3.0 (por ejemplo, **C:\EKM_Files** en Windows o **/opt/EKM_Files** en Linux).
2. Asegúrese de que la herramienta **keytool** de Java SDK esté disponible en la ruta de acceso de la línea de comandos.
3. Ejecute el comando siguiente para enumerar el contenido de la clasificación de claves de EKM 2.X:

   ```
   keytool -list -keystore <nombre_clasificación_claves_EKM_2.X> -storetype JCEKS
   ```

   donde <*EKM_2.X_keystore_name*> es el nombre de la clasificación de claves de EKM 2.X que está importando.

   Por ejemplo:

   keytool -list -keystore *EKMKeys.jck* -storetype JCEKS

   El sistema solicita una contraseña.
4. Introduzca la contraseña de la clasificación de claves de EKM 2.X y presione **Intro**.

   Se muestran el tipo de clasificación de claves de EKM 2.X, el certificado **ekmcert**, el proveedor de la clasificación de claves y las claves de la clasificación de claves de EKM 2.X. Esta lista se utilizará para comparación con la clasificación de claves de EKM 3.0 y verificar que estas claves no se encuentran en esta última.

NOTA: Mantenga abierto el símbolo del sistema. En un paso posterior, buscará estas claves o el certificado **ekmcert** en la clasificación de claves de EKM 3.0 para verificar que se han quitado de EKM 3.0.

5. Inicie el servidor de EKM 3.0 mediante el comando **startserver**. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.
6. *En un símbolo del sistema de Windows*, vaya a **<*root*>:\Dell\EKM\bin**. *En Linux*, vaya a **/opt/dell/ekm/bin**.
7. Conéctese al servidor de WebSphere mediante el comando **wsadmin**. Consulte Conexión al servidor de WebSphere.
8. En el símbolo del sistema **wsadmin**, utilice el alias de clave obtenido anteriormente y ejecute uno de los comandos siguientes para enumerar una clave o un certificado específico en el servidor EKM 3.0:

   Para claves:

   ```
   print AdminTask.tklmKeyList('[-alias <alias de la clave>]')
   ```

   Para el certificado **ekmcert**:

   ```
   print AdminTask.tklmKeyList('[-alias ekmcert]')
   ```

NOTA: Ha obtenido los alias de clave en un paso anterior. En Windows, puede copiar los alias mediante la barra de herramientas de la ventana del símbolo del sistema.

NOTA: Si desea comparar visualmente los alias de clave, puede enumerar todas las claves del servidor de EKM 3.0 al ejecutar el comando siguiente:

```
print AdminTask.tklmKeyList('[-alias]')
```

9. Presione **Intro**.

   Se ejecuta el comando.

   Si la clave duplicada no se encuentra en EKM 3.0, aparece el texto siguiente:

   ```
   Found 0 keys (Se han encontrado 0 claves).
   ```

   Si la clave o el certificado se encuentra en EKM 3.0, se muestran el UUID y el alias de la clave o el certificado.

Si la clave o el certificado se encuentra en EKM 3.0, elimínelos. Consulte Eliminación de una clave específica.

Repita este paso para cada clave duplicada que figura en la lista anterior.

7

Desinstalación de EKM 3.0

En este capítulo se describe cómo desinstalar EKM 3.0 en Windows y Linux.

PRECAUCIÓN: Si desinstala EKM 3.0, no se podrán leer los datos cifrados grabados en la biblioteca de cintas de Dell PowerVault a través del cifrado administrado por bibliotecas (LME). Asegúrese de restaurar todos los datos críticos antes de desinstalar EKM 3.0. Si existe la posibilidad de que vuelva a instalar EKM 3.0 en el futuro, cree una copia se seguridad antes de desinstalar EKM 3.0. Copie la copia de seguridad y el perfil de instalación de EKM 3.0 (si ha guardado un perfil de instalación) en una unidad externa antes de desinstalar EKM 3.0. Antes de volver a instalar EKM 3.0, utilice este archivo de copia de seguridad para realizar la operación de restauración. Consulte Creación de copias de seguridad y restauración desde una copia de seguridad.

NOTA: El proceso de desinstalación tarda aproximadamente 35 minutos. No apague el sistema hasta que se complete el proceso de desinstalación.

NOTA: Si desinstala EKM 3.0, también se desinstala WebSphere y DB2. Si utiliza DB2 para otras aplicaciones, Dell recomienda que no desinstale EKM 3.0. En su lugar, se recomienda detener el servicio de EKM 3.0. Para obtener información sobre cómo detener el servicio de EKM 3.0, consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux.

NOTA: Si tiene configurado un servidor principal/secundario, también deberá realizar el procedimiento de desinstalación en el servidor de EKM 3.0 secundario.

NOTA: Si quiere volver a instalar EKM 3.0, consulte Reinstalación de EKM 3.0.

Desinstalación de EKM 3.0 en Windows

Este procedimiento utiliza el programa de desinstalación de EKM 3.0 para Windows.

NOTA: El proceso de desinstalación tarda aproximadamente 35 minutos. No apague el sistema hasta que se complete el proceso de desinstalación.

1. En Windows 2008, abra el **Panel de control** y vaya a **Programas y características**.

   En Windows Server 2003 R2 con Service Pack 2, abra el **Panel de control** y vaya a **Agregar o quitar programas**.
2. Haga clic con el botón derecho del mouse en **EKM 3.0** y seleccione **Desinstalar**.
3. Siga las instrucciones que aparecen en pantalla.

   Una vez completada la desinstalación, aparecerá la ventana **Desinstalación finalizada**.
4. En la ventana **Desinstalación finalizada**, haga clic en **Listo**.

   Aparecerá un cuadro de diálogo indicando que se reiniciará el sistema.
5. En el cuadro de diálogo, haga clic en **Listo**. (Si no hace clic en **Listo**, Windows aún se reiniciará después de aproximadamente un minuto).

NOTA: Si Windows no se reinicia, reinicie el ordenador manualmente.

NOTA: Si encuentra errores durante el proceso de desinstalación, puede ver el registro de instalación principal en el directorio de inicio del usuario en **<*root*>:\Users\Administrator**. El archivo de registro de instalación es **IA--TIPxxx**. Desplácese hasta el final del archivo de registro de instalación principal para determinar dónde se detuvo el proceso o dónde se produjo el último error. También puede ver los registros de archivo en **<*root*>:\tklmv2properties** para obtener más detalles.

NOTA: Si está reinstalando EKM 3.0 y la instalación falla debido a una desinstalación incompleta, realice la desinstalación manualmente. Consulte Desinstalación manual de EKM 3.0 en Windows.

Desinstalación de EKM 3.0 en Linux

Este procedimiento utiliza el programa de desinstalación de EKM 3.0 para Linux.

NOTA: El proceso de desinstalación tarda aproximadamente 35 minutos. No apague el sistema hasta que se complete el proceso de desinstalación.

1. Abra una sesión de terminal y vaya a **/opt/dell/ekm/Uninstall_EKM**.
2. Ejecute **Uninstall EKM** (Desinstalar EKM). Para ello, ejecute el comando siguiente:
   ```
   ./Uninstall EKM
   ```
   Aparecerá una ventana emergente.
3. Haga clic en **Run** (Ejecutar) en la ventana emergente.
   Aparece la ventana **Uninstall EKM** (Desinstalar EKM).
4. Haga clic en **Uninstall** (Desinstalar).
   Se ejecuta el proceso de desinstalación.
5. Una vez completada la desinstalación, aparecerá la ventana **Uninstall Complete** (Desinstalación finalizada). Haga clic en **Done** (Listo).
   El sistema se reinicia.

NOTA: Si está reinstalando EKM 3.0 y la instalación falla debido a una desinstalación incompleta, realice la desinstalación manualmente. Consulte Desinstalación manual de EKM 3.0 en Linux.

8

Solución de problemas

En este capítulo se proporciona información sobre la solución de problemas, las preguntas frecuentes, los mensajes de error comunes y la información de contacto de asistencia técnica.

NOTA: Si el problema no se cubre en este capítulo, consulte la guía de solución de problemas de TKLM. Para obtener información sobre cómo acceder a la documentación de TKLM, consulte la sección sobre documentación y material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Cómo ponerse en contacto con Dell

NOTA: Si no dispone de una conexión a Internet activa, puede encontrar información de contacto en la factura de compra, en el albarán o en el catálogo de productos de Dell.

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio al cliente:

1. Vaya a **support.dell.com**.
2. Seleccione la categoría de soporte.
3. Si no es usted un cliente de EE.UU., seleccione su código de país en la parte inferior de la página o seleccione **Todos** para ver más posibilidades.
4. Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

Comprobaciones sobre los requisitos previos del sistema

EKM 3.0 realiza comprobaciones sobre los requisitos previos del sistema. Si recibe un mensaje de error después de la pantalla **License Agreement** (Contrato de licencia), siga las instrucciones del mensaje de error. Para conocer los errores más comunes y obtener las instrucciones relacionadas, consulte los elementos a continuación.

Fallo de los requisitos mínimos del sistema

si recibe el error **Minimum System Requirements Failed** (Fallo de los requisitos mínimos del sistema), haga clic en **Cancel and Exit** (Cancelar y salir) y confirme que el sistema cumple los requisitos. Consulte Requisitos de hardware y software.

El usuario no es un administrador en este sistema

Debe ser un usuario raíz en Linux o un administrador en Windows para instalar EKM 3.0.

SELinux debe estar desactivado

Si SELinux está instalado y activado, desactívelo antes de iniciar la instalación.

Para desactivar SELinux en RHEL5, realice los pasos siguientes:

1. En la barra de herramientas superior del escritorio, vaya a **Sistema** → **Administración** → **Nivel de seguridad y servidor de seguridad**.
   Aparecerá la ventana **Configuración de nivel de seguridad**.
2. Haga clic en la ficha **SELinux**. En el cuadro **Configuración de SELinux**, haga clic en las flechas y seleccione **Desactivado**.
3. Haga clic en **Aplicar**.
4. Haga clic en **Aceptar**.
5. Reinicie el sistema para que se efectue el cambio.

Para desactivar SELinux en RHEL4, realice los pasos siguientes:

1. Vaya a **Aplicaciones** → **Configuración del sistema** → **Nivel de seguridad** .
   Aparecerá una ventana emergente.
2. En la ventana emergente, seleccione la ficha **SELinux**.
3. En el menú desplegable, seleccione **Disable** (Desactivar).
4. Reinicie el sistema.

compat-libstdc++ no instalado

Si aparece el mensaje "compat-libstdc++ Not Installed" (compat-libstdc++ no instalado), consulte compat-libstdc++ no instalado.

Fallo de los requisitos de límites mínimos de memoria compartida

Al instalar EKM 3.0 en Linux, aparece el error siguiente:

```
The system did not meet the minimum shared memory requirements needed for the
installation. Make sure your system meets the minimum requirements before
attempting this installation (El sistema no cumple los requisitos mínimos de
memoria compartida que se necesitan para la instalación. Asegúrese de que el
sistema cumple los requisitos mínimos antes de intentar realizar la
instalación).
```

Para solucionar este problema, realice el procedimiento siguiente:

1. Para aumentar la memoria compartida al tamaño requerido y hacer que sea persistente, abra una sesión de terminal y ejecute el comando siguiente:

   ```
   echo "kernel.msgmni = 1024" >> /etc/sysctl.conf echo "kernel.msgmax =
   65536" >> /etc/sysctl.conf echo "kernel.msgmnb = 65536" >> /etc/sysctl.conf
   echo "kernel.sem = 250 256000 32 1024" >> /etc/sysctl.conf echo
   "kernel.shmmax = 1268435456" >> /etc/sysctl.conf
   ```

NOTA: Estos son los valores mínimos necesarios para instalar EKM 3.0 en Linux. Es posible que EKM 3.0 necesite más memoria compartida (kernel.shmmax) para que se instale correctamente. Si falla la instalación, desinstale EKM 3.0, aumente kernel.shmmax en un 25% y vuelva a instalar EKM 3.0. Para desinstalar EKM 3.0, consulte Desinstalación de EKM 3.0.

2. Ejecute el comando siguiente para que el sistema utilice el nuevo tamaño de memoria compartida inmediatamente (de lo contrario, deberá reiniciar):

   ```
   sysctl -p
   ```

El usuario de DB2 ya existe como un usuario regular

El nombre de usuario proporcionado para el campo **DB2 User Name** (Nombre de usuario de DB2) ya existe como un usuario en el sistema. Elija otro nombre.

TKLM o EKM 3.0 existente del mismo sistema

TKLM o EKM 3.0 ya está instalado. Desinstale la instancia existente o instale EKM 3.0 en otro sistema.

DB2 existente en el mismo sistema

DB2 ya está instalado. Desinstale DB2 o instale EKM 3.0 en otro sistema.

ksh no instalado

El instalador EKM 3.0 necesita **ksh**. Instale **ksh** y luego instale EKM 3.0. Consulte la documentación del sistema operativo.

El nombre de host tiene caracteres especiales

El nombre de host del sistema en el que está instalado EKM 3.0 no debe contener espacios ni caracteres especiales, tales como guiones (-) o guiones bajos (_). EKM 3.0 solo admite caracteres alfanuméricos en el nombre de host.

Nombre de dominio

El nombre de dominio del sistema en el que está instalado EKM 3.0 no debe contener espacios ni caracteres especiales, tales como guiones (-) o guiones bajos (_). EKM 3.0 solo admite caracteres alfanuméricos en el nombre de dominio.

Archivo /etc/hosts no válido

El archivo **/etc/hosts** debe contener una entrada válida para la dirección IPv4 de bucle de retroceso. La entrada debe tener el formato siguiente:

<Loopback IPv4 address><space><fully-qualified hostname><space><short hostname>

Donde <*space*> indica un espacio en blanco.

Códigos de error

Para obtener acceso a una lista de códigos de error y sus descripciones, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Archivos de referencia de Windows

Puede utilizar los siguientes archivos de registro y de error para realizar la solución de problemas que surjan durante la instalación de EKM 3.0 en Windows:

- **C:\tklm_install.stderr** (archivo de registro de errores estándar)
- **C:\tklmV2properties*.log** (archivos de registro de instalación de DB2)
- **C:\Users\Administrator\IA-TIPInstall-00.txt** (archivo de registro de instalación de EKM 3.0)

NOTA: Esta ruta de acceso se aplica a Windows Server 2008. Para Windows Server 2003 R2 con Service Pack 2, el archivo de registro de instalación de EKM 3.0 se encuentra en **C:\Documents and Settings\Administrator\IA--TIPInstall-00.txt**.

- **C:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt** (archivo de auditoría). Este archivo también se puede utilizar para la solución de problemas de uso, además de los problemas de instalación.

NOTA: En las rutas de acceso anteriores se supone que C: es la unidad raíz. Sustituya la letra de la unidad raíz con **C:**.

Archivos de referencia de Linux

Puede utilizar los siguientes archivos de registro y de error para realizar la solución de problemas que surjan durante la instalación de EKM 3.0 en Linux:

- **/root/IA-TipInstall_*.log**
- **/tklm_install.stderr** (archivo de registro de errores estándar)
- **/tklmV2properties/*.log**
- **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**

Desinstalación manual de EKM 3.0

Al desinstalar EKM 3.0, utilice primero el procedimiento de desinstalación automatizado. Consulte Desinstalación de EKM 3.0. Si falla el proceso de desinstalación automatizado, desinstale EKM 3.0 manualmente.

Desinstalación manual de EKM 3.0 en Windows

Si está reinstalando EKM 3.0 y la instalación falla debido a una desinstalación incompleta, realice una desinstalación manual. Si algún elemento ya se ha desinstalado, omita este paso.

NOTA: Si tiene la opción de reinstalar el sistema operativo del servidor, Dell recomienda que vuelva a instalar el sistema operativo y luego instale EKM 3.0.

NOTA: Las rutas de acceso de este procedimiento corresponden a Windows Server 2008. Cuando corresponda en el procedimiento, para Windows Server 2003 R2 con Service Pack 2, vaya a **Inicio** → **Panel de control** → **Agregar o quitar programas** .

1. Vaya a **Inicio** → **Panel de control** → **Programas (o Programas y funciones)** → **Desinstalar un programa** . Desinstale IBM DB2 (**DB2 Workgroup Server Edition - DB2TKLMV2**).
2. Vaya a **Inicio** → **Panel de control** → **Programas (o Programas y funciones)** → **Desinstalar un programa** .
3. Haga clic en **EKM**.
4. Haga clic en **Desinstalar o cambiar**.

   Aparece el asistente de desinstalación de EKM 3.0.
5. Siga las instrucciones del asistente de desinstalación.

   Una vez que EKM 3.0 se haya desinstalado, el sistema se reinicia automáticamente.
6. Vaya a **Inicio** → **Panel de control** → **Programas** → **Desinstalar un programa**. Desinstale **IBM Update Installer for WebSphere software V7.0**.
7. Ejecute el programa Editor del Registro de Windows (Regedit). Vaya a **HKEY_CURRENT_USER** → **Software** → **IBM** → **DB2** → **InstalledCopies**. Elimine la carpeta **DB2TLKMV2**.

PRECAUCIÓN: Tenga cuidado a la hora de editar el Registro. Si realiza un cambio incorrecto, el sistema podría hacerse inestable.

8. En Explorador de Windows, vaya a **<*root*>:\Dell**, si está presente (por ejemplo, **C:\Dell**). Elimine la carpeta **EKM** (si existe) y todas las subcarpetas que contiene (**<*root*>:\Dell\EKM**).
9. En la unidad raíz (por ejemplo, **C:**), elimine la carpeta **tklmV2properties** (**<*root*>:\tklmV2properties**).
10. En la unidad raíz, elimine la carpeta **tklmdbarchive**. (**<*root*>:\tklmdbarchive**).
11. En la unidad raíz, elimine la carpeta con el mismo nombre que el nombre de usuario de DB2.
12. En la unidad raíz, elimine el archivo **tklm_install.stderr** (**<*root*>:\tklm_install.stderr**).
13. En Explorador de Windows, vaya a **<*root*>:\Archivos de programa (x86)\dell**. Elimine el directorio de instalación de DB2 (**<*root*>:\Archivos de programa (x86)\dell\db2dkm**).

NOTA: En este paso y los tres pasos subsiguientes, si el sistema operativo es 32 bits, reemplace "Archivos de programa (x86)" con "Archivos de programa".

14. En Explorador de Windows, vaya a **<*root*>:\Archivos de programa (x86)\ibm**. Elimine la carpeta **Common** (**<*root*>:\Archivos de programa (x86)\ibm\Common**).
15. En Explorador de Windows, vaya a **<*root*>:\Archivos de programa (x86)\ibm**. Elimine la carpeta **gsk8** (**<*raíz*>:\Archivos de programa (x86)\ibm\gsk8**).
16. Vaya a **Inicio** → **Herramientas administrativas** → **Administración de equipos** . En el panel izquierdo, vaya a **Usuarios y grupos locales** → **Usuarios** . En el panel derecho, elimine las cuentas de administrador de DB2.

17. Vaya a **Inicio** → **Herramientas administrativas** → **Administración de equipos** . En el panel izquierdo, vaya a **Usuarios y grupos locales** → **Grupos** . En el panel derecho, elimine los grupos de administrador de DB2 (**DB2ADMINS** y **DB2USERS**).
18. En Explorador de Windows, vaya a **<*root*>:\Usuarios**. Elimine la carpeta con el mismo nombre que el nombre de usuario de DB2.
19. En Explorador de Windows, vaya a **<*root*>:\Usuarios\Administrator**. Elimine el archivo de texto **IA-TIPInstall-xx log**.
20. Detenga y elimine cualquiera de los siguientes servicios de Windows de EKM 3.0 instalados. Para ello, ejecute los comandos siguientes en el símbolo del sistema en la unidad raíz (por ejemplo, **C:**). Si el servicio ya está detenido, puede omitir el paso "detener".

NOTA: Si lo desea, puede detener y eliminar los servicios desde la utilidad de servicios de Windows.

```
sc stop "DBTKLM20" sc delete "DBTKLM20" sc stop "<DB2 user name>" sc delete
"<DB2 user name>" sc stop "DB2GOVERNOR_DB2TKLMV2" sc delete
"DB2GOVERNOR_DB2TKLMV2" sc stop "DB2LICD_DB2TKLMV2" sc delete
"DB2LICD_DB2TKLMV2" sc stop "DB2MGMTSVC_DB2TKLMV2" sc delete
"DB2MGMTSVC_DB2TKLMV2" sc stop "DB2REMOTECMD_DB2TKLMV2" sc delete
"DB2REMOTECMD_DB2TKLMV2" sc stop "DB2DAS00" sc delete "DB2DAS00"
```

NOTA: El servicio siguiente se muestra como **Tivoli Integrated Portal - TIPProfile_Port_<*DB2 port number*>** en la utilidad de servicios de Windows.

```
sc stop "IBMWAS61Service - TIPProfile_Port_<DB2 port number>" sc delete
"IBMWAS61Service - TIPProfile_Port_<DB2 port number>"
```

NOTA: El valor predeterminado del puerto de DB2 es 16310.

21. Ejecute los comandos siguientes en el símbolo del sistema en la unidad raíz (por ejemplo, **C:**):

```
reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Products
\907E425044C581845A83FCBED0CD5771 /f reg delete HKEY_LOCAL_MACHINE\software
\classes\installer\Features\907E425044C581845A83FCBED0CD5771 /f
```

22. Reinicie el sistema.
23. Si quiere volver a instalar EKM 3.0, consulte Procedimiento de instalación de EKM 3.0.

Desinstalación manual de EKM 3.0 en Linux

Si está reinstalando EKM 3.0 y la instalación falla debido a una desinstalación incompleta, realice una desinstalación manual. Si algún elemento ya se ha desinstalado, omita este paso.

NOTA: Si tiene la opción de reinstalar el sistema operativo del servidor, Dell recomienda que vuelva a instalar el sistema operativo y luego instale EKM 3.0.

En el procedimiento siguiente, reemplace las variables siguientes (<*variable*>) con las rutas de instalación o los nombres de variable de su sistema.

- <*DIR_INSTALACIÓN_DB2*>: el directorio seleccionado para la instalación de la base de datos.
- <*ADMIN_DB2*>: el ID del administrador de DB2 (por ejemplo, **ekm_dell1**).
- <*INICIO_ADMIN_DB2*>: el directorio de inicio de la base de datos (también conocido como la ubicación de datos de la base de datos).
- <*NOMBRE_BD_DB2*>: el nombre de la base de datos.

1. Abra una sesión de terminal.
2. Ejecute los comandos siguientes para quitar la instancia de DB2:

```
cd /opt/dell/ekm/products/tklm/_uninst ./removeDB2Inst.sh
<DIR_INSTALACIÓN_DB2> ./removeDB2Inst.sh <ADMIN_DB2> ./removeDB2Inst.sh
<INICIO_ADMIN_DB2> ./removeDB2Inst.sh <NOMBRE_BD_DB2>
```

Por ejemplo:

```
./removeDB2Inst.sh /opt/dell/db2ekm ./removeDB2Inst.sh /ekm_dell1 ./
removeDB2Inst.sh /home/db2ekm ./removeDB2Inst.sh /db2ekm
```

3. Ejecute la desinstalación silenciosa de TKLM con el archivo de respuesta. Para ello, ejecute los comandos siguientes:

   ```
   /opt/dell/ekm/_uninst/TIPInstall/uninstall -i silent –f /opt/dell/ekm/
   Uninstall_EKM/dkm_uninstall_response.txt
   ```

4. Ejecute los comandos siguientes para quitar los archivos de registro:

   ```
   rm –rf /tklmV2properties cd /opt/dell/ekm/ rm tklm_install.stderr rm IA-
   -TIPIn*.log rm EKM_Install*.log
   ```

5. Ejecute el comando siguiente para quitar el ID de usuario de DB2 del sistema:

   ```
   userdel -r $ADMIN_DB2$
   ```

   Por ejemplo:

   ```
   userdel -r ekm_dell1
   ```

6. Ejecute los comandos siguientes para quitar DB2 del sistema:

   ```
   cd /opt/dell/ekm/install ./db2_deinstall -a
   ```

7. Quite el directorio principal que se utiliza para la combinación/migración de EKM 2.X y la instalación de EKM 3.0.

   ```
   rm –rf /opt/dell/ekm
   ```

8. Reinicie el equipo.
9. Si quiere volver a instalar EKM 3.0, consulte Procedimiento de instalación de EKM 3.0.

Reinstalación de EKM 3.0

Para reinstalar EKM 3.0, realice los pasos siguientes:

1. Desinstale EKM 3.0 según el procedimiento de desinstalación. Consulte Desinstalación de EKM 3.0.

NOTA: Si el equipo no se reinicia automáticamente tras desinstalar EKM 3.0, reinícielo.

2. Reinstale EKM 3.0 según el procedimiento de instalación. Consulte Realización del procedimiento de instalación de EKM 3.0.

NOTA: Si ha guardado un perfil de instalación durante la instalación original de EKM 3.0, puede utilizarlo para reinstalar EKM 3.0. Sin embargo, si utiliza una configuración de servidor principal/secundario y el perfil de instalación pertenece al servidor secundario de EKM 3.0, no lo utilice para reinstalar EKM 3.0 en el servidor principal.

Preguntas más frecuentes

¿Puedo instalar EKM 3.0 en un sistema operativo que no figura en el capítulo Requisitos de hardware y software?

No. EKM 3.0 solo admite los sistemas operativos, las versiones, las ediciones, los niveles de Service Pack y los niveles de bits que se indican en Requisitos de hardware y software.

¿Puedo copiar archivos desde el instalador de EKM 3.0 en un disco duro en mi sistema e instalarlo desde mi sistema local?

No. EKM 3.0 solo admite la instalación desde el soporte de EKM 3.0. Consulte Instalación de EKM 3.0.

Durante la instalación de EKM 3.0, ¿qué debo hacer cuando recibo un mensaje de error que indica que ha fallado la instalación silenciosa?

Consulte el archivo **tklm_install.stderr** (archivo de registro de errores estándar) para obtener más información. *En Windows*, este archivo se encuentra en **<*root*>:\tklm_install.stderr**. *En Linux*, se encuentra en **/tklm_install.stderr**. Si figura un código de error en este archivo, consulte Códigos de error.

Cuando haya resuelto la situación de error que describe el código de error, realice una desinstalación manual. Consulte Desinstalación manual de EKM 3.0. Reinicie el sistema después de haber desinstalado manualmente EKM 3.0 y reinstale EKM 3.0.

Durante la reinstalación de EKM 3.0, ¿qué debo hacer cuando recibo un mensaje de error que indica que ha fallado la instalación?

Realice una desinstalación manual. Consulte Desinstalación manual de EKM 3.0. Reinicie el sistema después de haber desinstalado manualmente EKM 3.0 y reinstale EKM 3.0.

Durante la instalación de EKM 3.0, ¿qué debo hacer cuando recibo un mensaje de error que indica que no tengo Windows Server 2003 R2 SP2 instalado?

Para obtener una lista de sistemas operativos admitidos, consulte Requisitos de hardware y software. Después de haber instalado el segundo CD de Windows Server 2003 R2, reinicie el sistema antes de instalar EKM 3.0.

PRECAUCIÓN: Esta operación sobrescribirá los datos en el soporte de cinta. Una vez sobrescritos, los datos del soporte de cinta dejarán de ser accesibles.

¿Cómo vuelvo a utilizar el soporte cifrado anteriormente o el soporte no cifrado con una clave de cifrado diferente?

Volver a utilizar el soporte cifrado anteriormente requiere el uso de una configuración EKM 3.0 en funcionamiento que contenga claves para las cintas que se deben volver a utilizar y un PowerVault TL2000 o TL4000.

No puede sobrescribir las cintas de este modo en el PowerVault ML6000. Puede migrar cintas de un ML6000 a un TL2000 o TL4000 para este propósito. A continuación, deberá direccionar al TL2000 o TL4000 al servidor de EKM 3.0 adecuado.

Para volver a utilizar el soporte cifrado anteriormente, realice los pasos siguientes:

1. Asegúrese de que el servidor EKM 3.0 esté en ejecución y se haya configurado correctamente.
2. Conéctese a la GUI de RMU para el TL2000/TL4000 (se requiere una conexión de administrador/servicio).
3. Vaya a **Configure Library** (Configurar biblioteca).
4. Vaya a **Encryption** (Cifrado).
5. Cambie la configuración de **Encryption Policy** (Política de cifrado) a **Internal Label – Selective Encryption** (Etiqueta interna: cifrado selectivo).
6. Envíe un trabajo de escritura (por ejemplo, borrado rápido, borrado largo o copia de seguridad) al soporte que se debe reutilizar.

Para verificar que el cifrado se ha sobrescrito, realice los pasos siguientes:

1. Conéctese a la GUI de RMU para el TL2000/4000.
2. Vaya a **Monitor Library** (Supervisar biblioteca) y, a continuación, a **Inventory** (Inventario).
3. Haga clic en el menú desplegable de la revista adecuada.
4. Verifique que la sección **Comment** (Comentario) muestra **Not Encrypted** (No cifrado).

Puede quitar o desinstalar EKM 3.0 solamente después de que se hayan sobrescrito todos los soportes. Dell recomienda que realice una copia de seguridad de los archivos críticos de la GUI de EKM 3.0 y en un origen externo, tal como una unidad extraíble. Esto permite restaurar a EKM 3.0 en el caso de que sea necesario sobrescribir cintas adicionales.

Estoy teniendo problemas con una nueva instalación de EKM 3.0 y necesito volver a instalarlo. ¿Cómo puedo determinar si EKM 3.0 ha proporcionado claves?

1. Abra un símbolo del sistema y vaya al directorio de archivos de registros de auditoría.
   En Windows, el registro de auditoría se encuentra en **<*root*>:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt**.
   En Linux, el registro de auditoría se encuentra en: **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**.
2. Copie el archivo de registro de auditoría actual a un archivo temporal para que se pueda abrir. El archivo de registro de auditoría actual está activo y no se puede abrir durante la actualización.

3. Abra la copia temporal en un editor de texto (por ejemplo, WordPad). Busque **Drive Serial Number** (Número de serie de la unidad). Si hay una entrada, se ha proporcionado una clave. Si la entrada **volser** está en blanco, es el resultado de los diagnósticos de la ruta de acceso a la clave y debería buscar en el archivo para ver si hay entradas adicionales asociadas con el número de serie de la unidad.

PRECAUCIÓN: Si se han proporcionado claves, deberán descifrarse los datos en el soporte afectado antes de desinstalar EKM 3.0.

¿Cómo se verá afectada mi aplicación de copia de seguridad cuando configuro la biblioteca de cintas para el cifrado administrado por bibliotecas?

Cuando tenga activado el cifrado administrado por bibliotecas en la biblioteca de cintas y haya configurado particiones habilitadas para el cifrado, los cambios en la configuración de cintas se realizan en las unidades de dichas particiones. Debe detener y reiniciar los servicios de aplicación de copia de seguridad después de que las particiones habilitadas para el cifrado estén configuradas para asegurarse de que la aplicación de copia de seguridad reconoce la configuración de cifrado en las unidades.

NOTA: La aplicación de copia de seguridad en cintas no mostrará el cifrado en **enabled** (activado) si se utiliza el cifrado administrado por bibliotecas. La biblioteca de cintas mostrará las particiones como **encryption enabled** (habilitado para el cifrado). El cifrado administrado por bibliotecas es transparente para la aplicación de copia de seguridad de cintas. Esta última solo muestra el cifrado como **enabled** (activado) (por ejemplo, Symantec, CommVault, etc.) si la aplicación proporciona las claves de cifrado a las unidades.

¿Cómo administra EKM 3.0 la adición de nuevas unidades o el reemplazo de una unidad defectuosa?

Puede agregar unidades nuevas o de reemplazo al servidor de EKM 3.0 a través de la detección automática o manual. Para agregar unidades a través de detección automática, consulte Adición de un dispositivo a un grupo de dispositivos.

Dell recomienda que utilice la detección automática porque el número de serie de 12 dígitos (número de serie de 10 dígitos más dos ceros a la izquierda) debe introducirse para agregar la unidad manualmente. Si la seguridad es un tema de preocupación, puede activar la detección automática y ejecutar copias de seguridad de prueba o diagnósticos de ruta de acceso a claves en la biblioteca de cintas para agregar las unidades necesarias a la tabla de unidades. A continuación, puede desactivar la detección automática para impedir que las unidades nuevas obtengan claves. Siempre que EKM 3.0 pueda autenticar la firma digital asignada a la unidad en fábrica, EKM 3.0 acepta la solicitud de claves. Las claves se agrupan en la clasificación de claves en grupos de claves y puede asociar estos últimos con las unidades nuevas/de reemplazo después de que se agreguen las unidades.

NOTA: Si desea agregar un dispositivo manualmente, consulte la documentación de TKLM. Para obtener información acerca de cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

¿De qué manera EKM 3.0 controla la adición de una biblioteca de cintas nueva o el reemplazo de una biblioteca de cintas defectuosa?

En el cifrado administrado por biblioteca, la biblioteca de cintas es solo un proxy. Puede agregar o reemplazar bibliotecas de cintas y proporcionar claves siempre que EKM 3.0 pueda autenticarse con la firma digital en la unidad. La biblioteca de cintas de reemplazo deberá autenticarse según la firma digital de la unidad. La biblioteca de cintas de reemplazo deberá tener licencia para el cifrado administrador por biblioteca y configurarse para usar con el EKM 3.0 existente.

¿De qué modo el cifrado afecta la compresión y viceversa?

Los datos se comprimen antes de cifrarse porque los datos cifrados no suelen ser comprimibles. Por tanto, la compresión no afecta de ningún modo al cifrado y viceversa.

¿El cifrado tiene un impacto en el rendimiento?

Puede que se produzca un ligero impacto de rendimiento con cifrado pero no debería provocar un aumento en la ventana de respaldo.

¿Cómo solicito y utilizo un certificado de terceros?

Cree una solicitud de certificado en EKM 3.0 y envíela a una autoridad de certificados. El certificado que esta devuelva podrá importarse en EKM 3.0 y utilizarse para proteger los datos en un dispositivo habilitado para el cifrado o para la comunicación SSL. Consulte la documentación de TKLM para obtener más información acerca de cómo generar una solicitud de certificado, importar el certificado devuelto y utilizarlo para el cifrado. Para obtener información sobre cómo obtener acceso a la documentación de TKLM, consulte la sección sobre la documentación y el material de referencia del archivo **ReadThisFirst.txt** en el soporte de instalación de EKM 3.0.

Problemas conocidos y las soluciones correspondientes

Problema: no se puede crear una copia de seguridad.

Descripción:

Usando Internet Explorer, intenta crear una copia de seguridad de la clasificación de claves. Cuando especifica una ubicación de copia de seguridad que no existe, no se crea la copia de seguridad.

Resolución:

Realice una de las acciones siguientes. Si la acción no funciona, realice otra de la lista:

- Active JavaScript en el explorador. Si utiliza Internet Explorer V8, active el modo de Vista de compatibilidad.
- Utilice otro explorador compatible. Consulte Requisitos de hardware y software para obtener más información.
- Especifique una carpeta existente. Si desea especificar una carpeta nueva, créela primero antes de crear la copia de seguridad.

Problema: se crean varias copias de seguridad a la vez.

Descripción:

Al intentar crear una copia de seguridad de la clasificación de claves, se crean varios archivos de copia de seguridad a la vez. Este problema se produce rara vez.

Resolución:

Todos los archivos de copia de seguridad tienen el mismo contenido. Puede utilizar cualquiera de estos archivos para la operación de restauración.

Problema: es necesario introducir la información de conexión dos veces.

Descripción:

Cuando EKM 3.0 agote el tiempo de espera (tras un tiempo de inactividad de aproximadamente 30 minutos), el primer intento para volver a conectarse en EKM 3.0 se rechaza y es necesario intentar conectarse una segunda vez.

Resolución:

Introduzca la información de conexión EKM 3.0 ambas veces.

Problema: el panel derecho está oculto parcialmente por el panel de navegación.

Descripción:

Utiliza Internet Explorer y está accediendo a la pantalla **Key and Device Management** (Administración de claves y dispositivos) de EKM 3.0. Seleccione el grupo de claves o una unidad de cinta y el panel derecho queda oculto parcialmente por el panel de navegación.

Resolución:

Realice uno de los siguientes pasos:

- Actualice la pantalla.
- Maximice el explorador.
- Utilice otro explorador compatible. Consulte Requisitos de hardware y software para obtener más información.

Problema: aparece el texto "Certificate Error" (Error de certificado) en la parte superior del navegador.

Descripción:

Utiliza Internet Explorer 8 en modo de Vista de compatibilidad. Importa un certificado de autoridad correctamente, pero el error **Certificate Error** (Error de certificado) aparece en la parte superior de la pantalla siguiente, junto a la barra de la dirección URL.

Resolución:

Realice uno de los siguientes pasos:

- Omita el error, ya que no afecta al rendimiento de EKM 3.0.
- Utilice otro explorador compatible (por ejemplo, Internet Explorer 6.X o Firefox). Consulte Requisitos de hardware y software.

Problema: la información no se puede ordenar en tablas.

Descripción:

El uso de los campos de filtro de la parte superior de las tablas de las pantallas **Administer Server Certificates** (Administrar certificados de servidor), **Backup and Restore** (Copia de seguridad y restauración) y **Credential Store** (Almacén de credenciales) no ordena los elementos en las tablas.

Resolución:

Haga clic en la fila de encabezado de cada columna para ordenar los elementos.

Problema: no se puede introducir una descripción de la copia de seguridad creada.

Descripción:

Cuando se utiliza Firefox en Windows, se genera una copia de seguridad pero no se puede introducir una descripción de la misma y se utiliza una descripción predeterminada.

Resolución:

Utilice una versión compatible de Internet Explorer. Consulte Requisitos de hardware y software para obtener más información.

Problema: algunas acciones en la GUI de EKM 3.0 provocan errores de secuencia de comandos en el explorador.

Descripción

Aparecen errores de secuencia de comandos en el explorador y la acción solicitada no se completa.

Resolución:

Realice una de las acciones siguientes. Si la acción no funciona, realice otra de la lista:

- Active JavaScript en el explorador. Si utiliza Internet Explorer V8, active el modo de Vista de compatibilidad.

NOTA: El modo de Vista de compatibilidad debe activarse después de conectarse a EKM 3.0.

- Utilice otro explorador compatible. Consulte Requisitos de hardware y software para obtener más información.

Problema: durante la desinstalación, la barra de progreso no muestra el progreso correcto.

Descripción

La barra de progreso de desinstalación no muestra el progreso adecuado. La barra pasa a aproximadamente el 30% durante el principio de la desinstalación y se queda estático durante el resto del proceso. Luego, mueve al 100% al final.

Resolución

Este problema es conocido y no indica un problema con la desinstalación.

PRECAUCIÓN: No reinicie el sistema ni salga de la desinstalación.

Problema: la configuración de la pantalla Key and Device Management (Administración de claves y dispositivos) no se aplican.

Descripción

En la pantalla Key and Device Management (Administración de claves y dispositivos), cuando se intenta cambiar la configuración para la comunicación con la unidad, no se aplica el cambio.

Resolución:

Después de cambiar la configuración de la comunicación con la unidad, detenga e inicie el servidor de EKM 3.0. Se aplicarán los cambios. Consulte Inicio y detención del servidor EKM 3.0 en Windows o Inicio y detención del servidor EKM 3.0 en Linux para obtener más información.

Problema: en un servidor de Windows 2008, tras completar la instalación de EKM 3.0, la bandeja del sistema muestra un icono verde asociado con el procedimiento de instalación.

Descripción

La bandeja del sistema muestra un icono verde.

Resolución

Este problema es conocido y no afecta a la capacidad de uso ni a la fiabilidad de EKM 3.0. Cuando se desconecte del sistema y vuelve a conectarse, el icono no aparece.

Problema: al configurar la instalación de EKM 3.0, algunos campos muestran "0".

Descripción

Al configurar la instalación de EKM 3.0, algunos campos muestran "0". Esto sucede cuando utiliza un perfil de instalación al instalar EKM 3.0 y dicho perfil no es válido o tiene campos que faltan.

Resolución

Confirme que está utilizando un perfil de instalación válido.

NOTA: Si rellena los campos manualmente, deberá asegurarse de que los datos coincidan exactamente con los de la instalación original. De lo contrario, el segundo servidor no se podrá utilizar como servidor de seguridad para el primer servidor.

Problema: al crear una copia de seguridad, aparece un mensaje de error "software exception" (excepción de software).

Descripción

Al generar una copia de seguridad, se recibe un mensaje de error que indica que se ha producido una excepción de software.

Resolución

EKM 3.0 tiene una limitación conocida en los servidores que tienen 24 o más CPUs. Debe instalar el fixpack universal más reciente de DB2 para resolver este problema.

NOTA: Para obtener más información, consulte las notas de publicación en **support.dell.com/manuals**. Vaya a **Software → Systems Management (Administración de sistemas) → Dell Encryption Key Manager** .

Problema: no se pueden agregar roles a un usuario recién creado al utilizar Internet Explorer V8.

Descripción

Al conectarse como administrador de EKM 3.0, crear un usuario nuevo y luego intentar agregar un rol a este último, aparece un mensaje de error de JavaScript y el rol no se agrega.

Resolución

Cree el usuario primero y luego agregue roles a este mediante la pantalla **Administrative User Roles** (Roles de usuario administrativo). Para obtener acceso a ella, en el panel de navegación vaya a **Users and Groups (Usuarios y grupos de usuarios) → Administrative User Roles (Roles de usuario administrativo)**. Este problema también se puede resolver si utiliza una versión compatible de Firefox.

Problema: al desinstalar EKM 3.0, se muestra un error "stack overflow exception" (excepción de desbordamiento de pilas de Java).

Descripción

Al desinstalar EKM 3.0, se muestra un error de Java.

Resolución

Desinstale EKM 3.0 manualmente. Consulte Desinstalación manual de EKM 3.0 para obtener más información.

Problema: el proceso de desinstalación de EKM 3.0 se ejecuta durante varias horas y no se completa.

Descripción

Al intentar desinstalar EKM 3.0, el proceso de desinstalación no se completa.

Resolución

Desinstale EKM 3.0 manualmente. Consulte Desinstalación manual de EKM 3.0 para obtener más información.

Instalación de la biblioteca compat-libstdc++

En las plataformas Linux, la biblioteca **compat-libstdc++-33-3.2.3-61** o posterior debe instalarse antes de instalar EKM 3.0.

Si recibe el error siguiente al instalar EKM 3.0 en Linux, deberá instalar **compat-libstdc++**:

```
Your operating system does not have the compat-libstdc++ packaged installed (El sistema operativo no tiene instalado el paquete compat-libstdc++).
```

Para instalar **compat-libstdc++**:

1. En una sesión de terminal, vaya al archivo RPM **compat-libstdc++** en la carpeta **EKMPREREQLIBS** del soporte de instalación de EKM 3.0. Para ello, ejecute el comando siguiente:
   ```
   cd /<ruta_al_dvd_de_instalación_de_EKM_3.0>/EKMPREREQLIBS
   ```
2. Ejecute el comando siguiente para instalar **compat-libstdc++**:
   ```
   rpm -ivh compat-libstdc++*.rpm
   ```

NOTA: Si aparece un mensaje de error en el que se indica el archivo RPM **compat-libstdc++** que intenta instalar entra en conflicto con **libstdc++-33** ya instalado), realice los pasos siguientes:

a. Ejecute el comando siguiente:
   ```
   rpm –e libstdc++-33
   ```
b. Ejecute el comando siguiente:
   ```
   rpm -ivh compat-libstdc++*.rpm
   ```