

# OpenManage Integration versión 7.0 para Microsoft System Center

Guía del usuario

## Notas, precauciones y advertencias

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

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

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

**Copyright © 2009 - 2017 Dell Inc. o sus filiales. Todos los derechos reservados.** Dell, EMC y otras marcas comerciales son marcas comerciales de Dell Inc. o sus subsidiarias. Puede que otras marcas comerciales sean marcas comerciales de sus respectivos propietarios.

# Contenido

<b>1 Introducción.....</b>	<b>7</b>
Características de OMIMSSC.....	7
<b>2 Acerca de los componentes de OMIMSSC.....</b>	<b>9</b>
<b>3 Acerca del Portal para administradores.....</b>	<b>10</b>
Modificación de las cuentas de la IG y de SCCM o SCVMM.....	10
Modificación de las credenciales en el portal de administración de OMIMSSC .....	10
Reparación de la extensión de consola de OMIMSSC para SCCM.....	11
Reparación de la extensión de consola de OMIMSSC para SCVMM.....	11
Reparación de la IG de OMIMSSC.....	11
<b>4 Inicio de OMIMSSC desde la consola de MSSC inscrita.....</b>	<b>12</b>
Configuración del navegador.....	12
Inicio de la extensión de consola de OMIMSSC para SCCM.....	12
Inicio de la extensión de consola de OMIMSSC para SCVMM.....	13
<b>5 Casos de uso.....</b>	<b>14</b>
Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCCM.....	14
Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCVMM.....	15
Implementación de sistemas operativos que no son de Windows mediante las extensiones de la consola de OMIMSSC.....	15
Aplicar actualizaciones en servidores.....	15
Configurar los componentes sustituidos.....	16
Exportar e importar perfiles de servidor.....	16
<b>6 Perfiles.....</b>	<b>17</b>
Acerca del perfil de credenciales.....	17
Perfiles de credenciales predefinidos.....	17
Creación de perfil de credenciales.....	18
Modificación de perfil de credenciales.....	18
Eliminación de un perfil de credenciales.....	19
Acerca del perfil de hipervisor.....	19
Creación de perfil de hipervisor.....	19
Modificación de un perfil de hipervisor.....	20
Eliminación de perfil de hipervisor.....	20
<b>7 Inicio de la configuración e implementación.....</b>	<b>21</b>
<b>8 Detección de servidores y sincronización con la consola de MSSC.....</b>	<b>23</b>
Acerca de la configuración del servidor de referencia.....	23
Detección de servidores en OMIMSSC.....	23

Detección de servidores en la extensión de la consola de OMIMSSC para SCCM.....	24
Detección de servidores en la extensión de la consola de OMIMSSC para SCVMM.....	24
Requisitos del sistema para los sistemas administrados .....	24
Descubrimiento de servidores mediante descubrimiento automático.....	25
Detección manual de servidores.....	25
Sincronización de las extensiones de la consola de OMIMSSC con el SCCM inscrito.....	26
Sincronización de la extensión de la consola de OMIMSSC con el SCVMM inscrito.....	26
Sincronización con MSSC inscrito.....	27
Resolución de errores de sincronización.....	27
Eliminación de servidores de OMIMSSC.....	27
Inicio de la consola de la iDRAC.....	28
<b>9 Licencias de OMIMSSC.....</b>	<b>29</b>
Opciones después de cargar las licencias.....	29
Archivo de licencia para adquisiciones nuevas.....	29
Licencias de apilamiento.....	30
Reemplazo de licencias .....	30
Reimportación de licencias.....	30
Importación de varias licencias.....	30
Cumplimiento.....	30
Actualización de licencias.....	30
Licencia de evaluación.....	30
Consumo de licencias en OMIMSSC después de la detección de servidores.....	30
Importación de licencias en OMIMSSC.....	31
Visualización de información detallada de licencias.....	31
<b>10 Plantilla operativa.....</b>	<b>32</b>
Preparación para la implementación.....	32
Creación de imagen ISO de WinPE.....	32
Secuencia de tareas.....	34
Edición de una secuencia de tareas.....	35
Creación de medios de arranque de Lifecycle Controller.....	35
Configuración de una ubicación predeterminada de recurso compartido para el medio de inicio de Lifecycle Controller.....	36
Creación de una ISP de inicio de medio de secuencia de tareas.....	36
Para trabajar con la implementación de sistemas operativos que no sean de Windows .....	37
Administración de Plantilla operativa.....	37
Creación de una Plantilla operativa.....	37
Visualización de plantillas de Plantilla operativa.....	40
Edición de una Plantilla operativa.....	40
Eliminación de una Plantilla operativa.....	41
Plantilla operativaplantilla operativaPlantilla operativa plantilla operativa.....	41
Implementación de Plantilla operativa.....	42
<b>11 Integración con Dell Repository Manager (DRM).....</b>	<b>43</b>

<b>12 Mantenimiento.....</b>	<b>44</b>
Acerca de las actualizaciones del firmware .....	44
Aplicación de actualizaciones en los servidores.....	45
Recuperación.....	54
Almacén de protección.....	54
Exportación de perfiles de servidor.....	55
Importación de perfil del servidor.....	55
Cómo aplicar el firmware y los ajustes de configuración.....	56
Recopilación de registros de LC.....	57
Visualización de registros de LC.....	58
Descripción del archivo.....	59
Exportación de inventario.....	59
<b>13 Visualización de información en OMIMSSC.....</b>	<b>60</b>
Visualizar trabajos.....	61
Administración de trabajos.....	61
<b>14 Solución de problemas.....</b>	<b>62</b>
La opción de implementación no aparece en la secuencia de tareas.....	62
Creación de grupos de chasis VRTX duplicados .....	63
El grupo de actualización de clúster vacío no se elimina durante el descubrimiento automático o la sincronización.....	63
Error de creación de origen de actualización.....	63
Error de actualización de firmware porque la de cola de trabajos está llena.....	63
Error de actualización del firmware en grupo actualización de clúster.....	64
Error al actualizar el firmware en 11.a generación de servidores.....	64
Error al actualizar el firmware utilizando la fuente de actualización de DRM .....	64
Error de un trabajo programado en un grupo de actualización.....	64
Error al aplicar la Plantilla operativa .....	64
Error de acceso al recurso compartido de CIFS mediante el nombre de host.....	65
Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema.....	65
Error al crear un repositorio durante una actualización del firmware.....	65
Error al eliminar un grupo de actualización personalizado.....	65
Error de visualización de trabajos y registros.....	65
Error al exportar registros de LC en formato CSV.....	66
Error al exportar perfiles de servidores .....	66
Error al mostrar el logotipo de Dell EMC en el Portal para administradores de OMIMSSC.....	66
Error al ver los registros de LC .....	66
Actualización del firmware en algunos componentes independientemente de la selección.....	66
Error de implementación de hipervisores.....	66
Error de implementación del hipervisor debido a archivos de controlador retenidos en el recurso compartido de biblioteca.....	67
Error en la implementación del hipervisor en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory.....	67
Credenciales incorrectas durante la detección.....	68

Problema de instalación de IG mientras se ejecutan varias instancias del instalador en el mismo servidor .....	68
La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas.....	68
La información de inventario más reciente no aparece incluso después una actualización del firmware.....	68
Error 21119 de SCVMM VMM al agregar servidores Active Directory.....	69
<b>15 Apéndice.....</b>	<b>70</b>
<b>16 Acceso a documentos desde el sitio de asistencia de Dell EMC.....</b>	<b>71</b>
Cómo ponerse en contacto con Dell.....	71

# Introducción

OpenManage Integration para Microsoft System Center (OMIMSSC) proporciona las integraciones del conjunto de productos de System Center que permiten la administración completa del ciclo de vida de los servidores Dell EMC usando la Integrated Dell Remote Access Controller (iDRAC) con Lifecycle Controller (LC).

OMIMSSC ofrece implementación de sistemas operativos, parches para hardware, actualización de firmware y mantenimiento del servidor. Con OMIMSSC, puede realizar la integración con Microsoft System Center Configuration Manager (SCCM) para administrar los servidores Dell EMC en el centro de datos tradicional, o utilizar la integración con Microsoft System Center Virtual Machine Manager (SCVMM) para administrar los servidores Dell EMC en entornos virtualizados y de nube.

En esta guía, se proporciona información sobre el uso del producto y todos los casos de uso del producto.

Para obtener más información sobre SCCM y SCVMM, consulte la documentación de Microsoft.

## Características de OMIMSSC

**Tabla 1. Características de esta versión**

Función	Descripción
Implementación de sistemas operativos que no sean de Windows	Compatibilidad con implementaciones de sistemas operativos que no sean de Windows (ESXi y RHEL).
Servidores PowerEdge de 14. <sup>a</sup> generación	Compatibilidad para detectar y administrar la 14. <sup>a</sup> generación de servidores Dell EMC PowerEdge.
Modo de bloqueo de la iDRAC	Compatibilidad con el modo de bloqueo de la iDRAC para la 14. <sup>a</sup> generación de servidores PowerEdge.
Multiconsola	Compatibilidad para la integración con varias consolas de SCCM y SCVMM con un solo dispositivo OMIMSSC.
Detección	Detección de servidores PowerEdge de 11. <sup>a</sup> generación y posteriores, e instalación en el entorno de Microsoft System Center (MSSC).
Sincronización con MSSC	Sincronización de todos los sistemas host de Dell EMC que aparecen en el entorno de SCCM o SCVMM inscrito con OMIMSSC.
Centro de licencias	Administración de licencias de OMIMSSC desde el Portal para administradores.
Inventario	Visualización de detalles clave del inventario relacionados con los servidores Dell EMC.
Configurar el hardware	Compatibilidad para configurar el adaptador de red, Fiber Channel y los componentes de PCIe y SSD de los servidores PowerEdge.
Creación de medio de arranque	Compatibilidad para crear un medio de arranque de implementación sin intervención a partir de una secuencia de tareas.

Plantilla operativa	Uso de una plantilla uniforme para la actualización de firmware, la configuración de hardware y la implementación del sistema operativo.
Cumplimiento de plantilla operativa	Comprobación del cumplimiento de la configuración de hardware en relación con la plantilla operativa.
Actualización compatible en clústeres (CAU) de Microsoft	Automatización del proceso de actualización del firmware mediante la función de CAU de Microsoft.
Exportar inventario	Después de comparar los inventarios de servidores con el origen de actualizaciones, puede exportar el informe comparativo en un archivo .CSV o .XML.
Exportar perfil del servidor	Exportación de un perfil de servidor, incluidas las imágenes de firmware en componentes como el sistema básico de entrada/salida (BIOS), el arreglo redundante de discos independientes (RAID), la controladora de interfaces de red (NIC), la iDRAC, el LC, etc., a una ubicación interna o externa.
Importar perfil del servidor	Importación de un perfil de servidor manteniendo o excluyendo la configuración actual del RAID.
Recopilar y ver los mensajes del registro de LifeCycle Controller (LC)	Exportación, visualización y descarga a un archivo .CSV, y búsqueda en los mensajes de registro de LC.
Sondeo y notificaciones	Configuración de notificaciones para recibir alertas cuando haya disponibles nuevos catálogos en el origen de actualizaciones.

## Acerca de los componentes de OMIMSSC

A continuación se muestra la lista de los componentes de OMIMSSC que han sido utilizados en esta guía y sus nombres:

- Máquina virtual Appliance de OpenManage Integration para Microsoft System Center, también conocida como Appliance. Se aloja en un hipervisor como máquina virtual basada en CentOS y realiza las tareas siguientes:
  - Interactúa con los servidores Dell EMC a través de iDRAC mediante comandos de Web Services-Management (WSMan).
  - Le permite administrar la MV Appliance de OMIMSSC a través del portal de administración.
- La puerta de enlace de integración de OMIMSSC, también conocida como IG, es un conjunto de servicios web instalado en el servidor Windows y realiza las tareas siguientes:
  - Ejecuta comandos Powershell de SCCM o SCVMM, y funciona como una puerta de enlace entre SCCM o SCVMM y Appliance.
  - Personaliza WinPE para Appliance.
- Consola de OpenManage Integration para Microsoft System Center, también conocida como la consola de OMIMSSC
  - Complemento de la consola de OMIMSSC para SCCM, también conocido como la extensión de consola de OMIMSSC para SCCM
  - Complemento de la consola de OMIMSSC para SCVMM, también conocido como la extensión de consola de OMIMSSC para SCVMM

# Acerca del Portal para administradores

El Portal para administradores le permite iniciar sesión en OMIMSSC como administrador para ver todos los trabajos iniciados en OMIMSSC por distintos usuarios, ver detalles de la licencia, detalles de la consola, descargar los componentes necesarios y actualizar OMIMSSC. A continuación, se describen los casos de uso en el Portal para administradores junto con las licencias.

Temas:

- [Modificación de las cuentas de la IG y de SCCM o SCVMM](#)
- [Reparación de la extensión de consola de OMIMSSC para SCCM](#)
- [Reparación de la extensión de consola de OMIMSSC para SCVMM](#)
- [Reparación de la IG de OMIMSSC](#)

## Modificación de las cuentas de la IG y de SCCM o SCVMM

Utilizando esta opción, puede cambiar las contraseñas de las cuentas de SCCM, de SCVMM y de la IG en la consola de OMIMSSC.

### Acerca de esta tarea

Desde el portal de administración, puede modificar las credenciales de administrador de SCCM o SCVMM y las credenciales de la IG. Este proceso es una actividad secuencial.

- Para la cuenta de la IG, respete los siguientes prerrequisitos antes de modificar la cuenta en OMIMSSC:
  - a Modifique las credenciales en Active Directory.
  - b Modifique las credenciales en el instalador de la IG.
- Para cuentas de SCCM o SCVMM, modifique las credenciales en Active Directory antes de modificar la cuenta en OMIMSSC.

Para modificar la cuenta de la IG de OMIMSSC desde el instalador:

### Pasos

- 1 Ejecute el instalador de la IG.
- 2 En **Mantenimiento de programas**, seleccione **Modificar** y haga clic en **Siguiente**.
- 3 Cambie la contraseña y, a continuación, haga clic en **Siguiente**.
- 4 En **Modificar el programa**, haga clic en **Instalar**.
- 5 Haga clic en **Finish (Finalizar)** una vez concluida la tarea de modificación.

## Modificación de las credenciales en el portal de administración de OMIMSSC

- 1 En el portal de administración de OMIMSSC, haga clic en **Settings (Configuración)** y, a continuación, haga clic en **Console Enrollment (Inscripción de consolas)**.  
Se mostrarán las consolas inscritas.
- 2 Seleccione una consola para editar y haga clic en **Edit (Editar)**.
- 3 Introduzca los nuevos detalles y haga clic en **Finish (Finalizar)** para guardar los cambios.

# Reparación de la extensión de consola de OMIMSSC para SCCM

Para reparar los archivos de OMIMSSC en el caso de que están dañados, siga estos pasos:

- 1 Ejecute el instalador de la extensión de consola de OMIMSSC para SCCM.  
Se muestra la pantalla de **Welcome (bienvenida)**.
- 2 Haga clic en **Next (Siguiete)**.
- 3 En **Mantenimiento de programas**, seleccione **Reparar** y haga clic en **Siguiete**.  
Aparecerá la pantalla **Ready to Repair the Program (Listo para reparar el programa)**.
- 4 Haga clic en **Instalar**.  
En la pantalla se verá el progreso de la instalación. Una vez finalizada la instalación, aparece la ventana **InstallShield Wizard Completed (Asistente InstallShield completado)**.
- 5 Haga clic en **Finalizar**.

# Reparación de la extensión de consola de OMIMSSC para SCVMM

Para reparar los archivos de OMIMSSC en el caso de que están dañados, siga estos pasos:

- 1 Ejecute el instalador de la **extensión de consola de OMIMSSC para SCVMM**.
- 2 En **Mantenimiento de programas**, seleccione **Reparar** y haga clic en **Siguiete**.
- 3 En **Ready to Repair or Remove the program (Listo para reparar o quitar el programa)**, haga clic en **Repair (Reparar)**.
- 4 Cuando finalice la tarea de reparación, haga clic en **Finish (Finalizar)**.

# Reparación de la IG de OMIMSSC

## Acerca de esta tarea

Mediante esta opción, puede volver a instalar los archivos dañados o eliminados, o volver a crear las carpetas necesarias para la IG de OMIMSSC.

## Pasos

- 1 Ejecute el instalador de la IG de OMIMSSC.
- 2 En **Mantenimiento de programas**, seleccione **Reparar** y haga clic en **Siguiete**.
- 3 En **Ready to Repair (Listo para reparar)**, proporcione la contraseña de la cuenta de usuario de la puerta de enlace de integración y, a continuación, haga clic en **Install (Instalar)**.
- 4 Haga clic en **Finish (Finalizar)** una vez concluida la tarea de reparación.

# Inicio de OMIMSSC desde la consola de MSSC inscrita

Inicie OMIMSSC desde la consola de SCCM o SCVMM inscrita.

Temas:

- [Configuración del navegador](#)
- [Inicio de la extensión de consola de OMIMSSC para SCCM](#)
- [Inicio de la extensión de consola de OMIMSSC para SCVMM](#)

## Configuración del navegador

### Acerca de esta tarea

Antes de iniciar OMIMSSC, agregue la dirección IP de OMIMSSC como un requisito previo en la lista de sitios de la **intranet local** para realizar las siguientes operaciones:

- exportar y visualizar el inventario de firmware
- ver registros de LC
- exportar los valores en grupo en la Plantilla operativa

Antes de descargar los archivos .CSV, realice estos pasos:

### Pasos

- 1 Haga clic en **IE Settings (Configuración de IE)** y, luego, haga clic en **Internet Options (Opciones de Internet)**.
- 2 Haga clic en **Advanced (Configuración avanzada)** y, en **Settings (Configuración)**, busque la sección **Security (Seguridad)**.
- 3 Cancele la selección de la opción **Do not save encrypted pages to disk (No guardar las páginas cifradas en el disco)** y haga clic en **OK (Aceptar)**.

## Inicio de la extensión de consola de OMIMSSC para SCCM

### Prerequisito

Inicie sesión en el SO Windows con las mismas credenciales empleadas para iniciar sesión en la extensión de consola de OMIMSSC para SCCM.

### Paso

En la consola de SCCM, haga clic en **Assets and Compliance (Recursos y cumplimiento)**, haga clic en **Overview (Descripción general)** y, a continuación, haga clic en la extensión de consola de **OMIMSSC para SCCM**.

① **NOTA:** Si se conecta a la consola de SCCM mediante el protocolo de escritorio remoto (RDP), la sesión de OMIMSSC puede finalizar si se cierra el RDP. Por lo tanto, vuelva a iniciar sesión después de volver a abrir la sesión de RDP.

## Inicio de la extensión de consola de OMIMSSC para SCVMM

1 En la consola de SCVMM, seleccione **Fabric (Red Fabric)** y, a continuación, seleccione los grupos de servidores **All Hosts (Todos los hosts)**.

① **NOTA:** Para indicar OMIMSSC, puede seleccionar cualquier grupo de hosts para el cual tenga permiso de acceso.

2 En la cinta **Home (Inicio)**, seleccione **OMIMSSC**.

## Casos de uso

Puede instalar el sistema operativo solo en los servidores cuya configuración de hardware es compatible con OMIMSSC. Antes de la implementación del sistema operativo, asegúrese de actualizar el firmware a las versiones más recientes disponibles en [ftp.dell.com](http://ftp.dell.com) o [downloads.dell.com](http://downloads.dell.com) y, luego, continúe con la implementación del sistema operativo. A continuación, se detallan algunas de las situaciones que tienen lugar cuando se usan extensiones de la consola de OMIMSSC:

Temas:

- Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCCM
- Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCVMM
- Implementación de sistemas operativos que no son de Windows mediante las extensiones de la consola de OMIMSSC
- Aplicar actualizaciones en servidores
- Configurar los componentes sustituidos
- Exportar e importar perfiles de servidor

## Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCCM

### Acerca de esta tarea

Para implementar sistemas operativos en servidores seleccionados, siga estos pasos:

### Pasos

- 1 Descargue la versión más reciente de Dell Deployment ToolKit (DTK) y cree una imagen ISO de arranque del entorno de preinstalación de Windows (WinPE). Para obtener más información, consulte la [actualización de WinPE](#).
- 2 Importe esta imagen .wim en la consola de SCCM y cree una imagen de arranque en SCCM. Para obtener más información, consulte la [documentación de Microsoft](#).
- 3 Cree una secuencia de tareas en SCCM. Para obtener más información, consulte [Creación de una secuencia de tareas](#).
- 4 Cree una imagen de secuencia de tareas en SCCM. Para obtener más información, consulte la [documentación de Microsoft](#).
- 5 Genere una imagen ISO desatendida. Para obtener más información, consulte [Creación de medio de arranque de LC](#).
- 6 Detecte un servidor de referencia mediante la página **Discovery (Detección)**. Para obtener más información, consulte [Detección manual de servidores](#).
- 7 Cree una Plantilla operativa. Para obtener más información, consulte [Creación de una plantilla operativa](#).
- 8 Asigne una Plantilla operativa. Para obtener más información, consulte [Asignación de una plantilla operativa](#).
- 9 Implemente una Plantilla operativa. Para obtener más información, consulte [Implementación de una plantilla operativa](#).

**NOTA:** Antes de implementar el sistema operativo en un servidor host, asegúrese de que el estado de Client (Cliente) del servidor sea No en SCCM.

**NOTA:** Después de implementar correctamente el sistema operativo Windows en el entorno de SCCM, el servidor no aparece como host en OMIMSSC. Para ver el servidor en la ficha de host, compruebe que el estado de Client (Cliente) del servidor sea YES (Sí) en SCCM y, luego, sincronice OMIMSSC con SCCM.

- 10 Vea el estado del trabajo de actualización del firmware y de visualización en pantalla (OSD) en la página **Jobs and Logs Center (Centro de trabajos y registros)**. Para obtener más información, consulte [Visualización de la información en OMIMSSC](#).

# Implementación del sistema operativo mediante la extensión de la consola de OMIMSSC para SCVMM

## Acerca de esta tarea

Para implementar sistemas operativos en los servidores seleccionados, siga estos pasos:

### Pasos

- 1 Descargue la versión más reciente de Dell Deployment ToolKit (DTK) y cree una imagen ISO de arranque del entorno de preinstalación de Windows (WinPE). Para obtener más información, consulte la [actualización de WinPE](#).
- 2 Cree un perfil de la computadora física en SCVMM. Para obtener más información, consulte la documentación de SCVMM.
- 3 Cree un grupo de hosts de destino en SCVMM. Para obtener más información, consulte la documentación de SCVMM.
- 4 Cree un perfil de hipervisor en la extensión de la consola de OMIMSSC para SCVMM. Para obtener más información, consulte [Creación de un perfil de hipervisor](#).
- 5 Detecte un servidor de referencia mediante la página **Discovery (Detección)**. Para obtener más información, consulte [Detección manual de servidores](#).
- 6 Cree una Plantilla operativa. Para obtener más información, consulte [Creación de una Plantilla operativa](#).
- 7 Asigne una Plantilla operativa. Para obtener más información, consulte [Asignación de una Plantilla operativa](#).
- 8 Implemente una Plantilla operativa. Para obtener más información, consulte [Implementación de una Plantilla operativa](#).

**Tabla 3. Diferentes escenarios para la implementación de hipervisores**

Si necesita los controladores de fábrica más reciente y los controladores fuera de banda	Al crear un perfil del hipervisor, active LC Driver Injection.
Si desea conservar la configuración de hardware existente	Al crear la Plantilla operativa, anule la selección de todos los componentes físicos.

- 9 Vea el estado del trabajo de actualización del firmware y de visualización en pantalla (OSD) en la página **Jobs and Logs Center (Centro de trabajos y registros)**. Para obtener más información, consulte [Visualización de la información en OMIMSSC](#).

# Implementación de sistemas operativos que no son de Windows mediante las extensiones de la consola de OMIMSSC

## Acerca de esta tarea

Para implementar cualquier tipo de sistema operativo que no sea de Windows, realice lo siguiente:

### Pasos

- 1 Cree una Plantilla operativa. Para obtener más información, consulte [Creación de una Plantilla operativa](#).
- 2 Asigne una Plantilla operativa. Para obtener más información, consulte [Asignación de una Plantilla operativa](#).
- 3 Implemente una Plantilla operativa. Para obtener más información, consulte [Implementación de una Plantilla operativa](#).

### NOTA:

Si ocurre un error en la búsqueda de DHCP durante la implementación, se agota el tiempo de espera en el servidor y no se traslada a la recopilación de **Managed Dell Lifecycle Controller (ESXi)** en SCCM.

# Aplicar actualizaciones en servidores

## Acerca de esta tarea

Puede actualizar los servidores o grupos de servidores seleccionados mediante los siguientes orígenes de actualizaciones:

- FTP en línea y origen de FTP local.

- HTTP en línea y HTTP local
- Repositorio Dell Repository Manager (DRM) local

### Pasos

- 1 Antes de comenzar con las actualizaciones, vea la información sobre orígenes y grupos de actualizaciones. Para obtener más información sobre orígenes de actualizaciones, consulte [origen de actualizaciones](#). Asegúrese de que haya un origen de actualizaciones creado. Para obtener más información, consulte [Creación de un origen de actualizaciones](#).
  - 2 Detecte o sincronice los servidores con MSSC registrado. Para obtener más información, consulte [Detección y sincronización de dispositivos](#). Asegúrese de que el inventario de servidores sea el más reciente. Para obtener más información, consulte [Inicio de la configuración e implementación](#).
  - 3 Actualice los servidores mediante una de las siguientes opciones:
    - Seleccione los grupos de servidores necesarios para aplicar las actualizaciones. Para obtener más información, consulte [Aplicación de actualizaciones en los servidores](#).
- NOTA: Seleccione Allow Downgrade (Permitir degradación) para degradar la versión de firmware de los componentes.**
- Utilice el componente de actualización del firmware en Plantilla operativa. Para obtener más información, consulte [Creación de una Plantilla operativa](#).
- 4 Modifique el origen de actualizaciones con el catálogo más reciente mediante sondeo y notificación. Para obtener más información, consulte [Sondeo y notificación](#).

## Configurar los componentes sustituidos

Para actualizar un componente de servidor sustituido a la versión de firmware requerida o la configuración de un componente antiguo (o ambos), consulte [Aplicar el firmware y los valores de configuración](#).

## Exportar e importar perfiles de servidor

Para exportar e importar un perfil de servidor:

- 1 Cree un almacén de protección. Para obtener más información, consulte [Creación de un almacén de protección](#).
- 2 Exporte un perfil de servidor. Para obtener más información, consulte [Creación de un trabajo de exportación](#).
- 3 Exporte un perfil de servidor que incluya la configuración del RAID e importe un perfil de servidor que incluya la configuración del RAID. Para obtener más información, consulte [Recuperación](#).

# Perfiles

Los perfiles le permiten administrar sus credenciales y personalizar imágenes WinPE para la implementación. Los diferentes tipos de perfiles admitidos en OMIMSSC son los siguientes:

Temas:

- [Acerca del perfil de credenciales](#)
- [Acerca del perfil de hipervisor](#)

## Acerca del perfil de credenciales

Los perfiles de credenciales simplifican el uso y la administración de credenciales de usuario mediante las capacidades de autenticación basada en roles del usuario. Cada perfil de credenciales contiene un nombre de usuario y la contraseña de una sola cuenta de usuario. Un perfil de credenciales autentica las capacidades basadas en roles de un usuario. El dispositivo utiliza perfiles de credenciales para conectarse con la iDRAC de los sistemas administrados.

Además, puede utilizar los perfiles de credenciales para acceder al sitio FTP y a los recursos disponibles en los recursos compartidos de Windows y al trabajar con diferentes funciones del iDRAC.

Puede crear cuatro tipos de perfiles de credenciales:

- Perfil de credenciales del dispositivo: este perfil se utiliza para iniciar sesión en el iDRAC o en Chassis Management Controller (CMC).
  - ⓘ **NOTA: Cuando no se crea ni selecciona ningún perfil predeterminado, se utiliza la configuración predeterminada de fábrica de la iDRAC. El nombre de usuario predeterminado es `root` y la contraseña es `calvin`.**  
El perfil del iDRAC predeterminado se utiliza para acceder al servidor cuando descubre un servidor o realiza una sincronización.
  - ⓘ **NOTA: El perfil de CMC predeterminado tiene el nombre de usuario `root` y la contraseña `calvin`, y se utiliza para acceder al servidor modular para obtener información sobre el chasis.**
  - ⓘ **NOTA: Utilice el perfil de credenciales de tipo de dispositivo para detectar un servidor, iniciar sesión en la CMC, resolver problemas de sincronización e implementar el sistema operativo.**
- Windows Credential Profile (Perfil de credenciales de Windows): Este perfil se utiliza para acceder a los recursos compartidos de Windows durante la creación de un origen de actualizaciones de DRM.
- FTP Credential Profile (Perfil de credenciales de FTP): Este perfil se utiliza para acceder al sitio FTP.
- Proxy Server Credentials (Credenciales del servidor proxy): Este perfil se utiliza para proporcionar credenciales de proxy que permitan acceder a los sitios FTP y obtener las actualizaciones.

## Perfiles de credenciales predefinidos

La cuenta **SYSTEM DEFAULT FTP (SISTEMA FTP PREDETERMINADO)** es un perfil de credenciales predefinido de tipo FTP con los campos **Username (Nombre de usuario)** y **Password (Contraseña)** definidos como **Anonymous (Anónimo)**. No se puede editar. Este perfil se utiliza para acceder a `ftp.dell.com`

# Creación de perfil de credenciales

## Acerca de esta tarea

Al crear un perfil de credenciales, tenga en cuenta lo siguiente:

- Cuando se crea un perfil de credenciales de tipo de dispositivo, se crea una **RunAsAccount (Cuenta de ejecución)** asociada en **SCVMM** para administrar el servidor y el nombre de **RunAsAccount** es `Dell_CredentialProfileName`.
- Durante la detección automática, si no hay ningún perfil de credenciales disponible para la iDRAC, se usará la configuración predeterminada de la iDRAC de fábrica. El nombre de usuario predeterminado es **root** y la contraseña es **calvin**.

## Pasos

- 1 En OMIMSSC, realice alguno de estos pasos para abrir el perfil de credenciales:
  - En el panel de OMIMSSC, haga clic en **Create Credential Profile (Crear perfil de credenciales)**.
  - En el panel de navegación, haga clic en **Profiles (Perfiles) > Credential Profile (Perfil de credenciales)** y, luego, haga clic en **Create (Crear)**.
- 2 En **Credential Profile (Perfil de credenciales)**, seleccione el tipo de perfil de credencial que desea utilizar. OMIMSSC admite cuatro tipos de perfiles de credenciales y hay uno predefinido. Puede crear los siguientes cuatro tipos de perfiles de credenciales:
  - **Device Credential Profile (Perfil de credenciales del dispositivo)**: Este perfil se utiliza para iniciar sesión en iDRAC o en Chassis Management Controller (CMC).
    - ① **NOTA:** Al crear el Device Credential Profile (Perfil de credenciales del dispositivo), seleccione iDRAC para que sea el perfil predeterminado de iDRAC o CMC para que sea el perfil predeterminado para Chassis Management Controller (CMC). Seleccione None (Ninguno) si elige no establecer este perfil como un perfil predeterminado.
    - Cuando se crea un perfil de credenciales de tipo de dispositivo, se crea una **RunAsAccount** asociada en **SCVMM** para administrar el servidor, y el nombre de la cuenta es `Dell_CredentialProfileName`.
      - Se recomienda no editar ni eliminar la **RunAsAccount**.
      - Si elimina el perfil de credenciales de tipo de dispositivo, la **RunAsAccount** asociada desde SCVMM también se eliminará. Por lo tanto, el perfil de credenciales correspondiente no estará visible en OMIMSSC.
    - **Windows Credential Profile (Perfil de credenciales de Windows)**: Utilice este perfil para acceder a las carpetas compartidas en Windows.
    - **FTP Credential Profile (Perfil de credenciales de FTP)**: Utilice este perfil para acceder al sitio FTP.
      - ① **NOTA:** El perfil de credenciales predeterminado de FTP que está disponible en el dispositivo es **System Default FTP (FTP predeterminado de sistema)**.
      - **SYSTEM DEFAULT FTP (FTP PREDETERMINADO DE SISTEMA)**: Perfil de credenciales predefinido para credenciales tipo FTP; el campo de contraseña no es obligatorio para este tipo.
      - **Proxy Server Credentials (Credenciales del servidor proxy)**: Utilice este perfil para proporcionar credenciales de proxy de los sitios FTP para las actualizaciones de firmware.
  - 3 En **Domain (Dominio)**, proporcione los detalles del dominio para las credenciales de Windows; en **Proxy Server URL (URL de servidor proxy)**, proporcione la URL del servidor proxy en el formato `http://hostname:port` o `http://IPaddress:port`; en **Default profile for (Perfil predeterminado para)**, seleccione este perfil como el perfil predeterminado para iniciar sesión en iDRAC o CMC. Seleccione **None (Ninguno)** si elige no establecer este perfil como un perfil predeterminado.
    - ① **NOTA:** La opción **Default Profile for (Perfil predeterminado para)** se aplica solamente al perfil de credenciales de tipo de dispositivo.
  - 4 Para crear el perfil, haga clic en **Finish (Finalizar)**.

# Modificación de perfil de credenciales

## Acerca de esta tarea

Tenga en cuenta lo siguiente al modificar un perfil de credenciales:

- No podrá modificar el tipo de perfil de credenciales después de crearlo. Sin embargo, puede modificar otros campos. Para ver las modificaciones, actualice la pantalla.
- No se puede modificar un perfil de credenciales de tipo de dispositivo si se está utilizando.
- No se puede modificar un perfil de credenciales si está en uso.

#### Pasos

- 1 Seleccione el perfil de credenciales que desee modificar, haga clic en **Edit (Editar)** y actualice el perfil.
- 2 Para guardar los cambios realizados, haga clic en **Save (Guardar)**.

## Eliminación de un perfil de credenciales

#### Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar un perfil de credenciales:

- Cuando se elimina un perfil de credenciales de tipo dispositivo, también se elimina la **Cuenta de ejecución** asociada de SCVMM.
- Cuando se elimina **RunAsAccount (Cuenta de ejecución)** en SCVMM, el perfil de credenciales correspondiente no está disponible en el dispositivo.
- Para eliminar el perfil de credenciales que se usa en detección de servidores, elimine la información del servidor detectado y, a continuación, elimine el perfil de credenciales.
- Para eliminar un perfil de credenciales de tipo de dispositivo que se utilice para la implementación, primero elimine los servidores implementados en el entorno de SCVMM y, luego, el perfil de credenciales.
- No puede eliminar un perfil de credenciales que se utilice en un origen de actualizaciones.

#### Paso

Seleccione el perfil de credenciales que desee eliminar y haga clic en **Delete (Eliminar)**.

## Acerca del perfil de hipervisor

Un perfil de hipervisor contiene una ISO de WinPE personalizada (esta ISO se utiliza para implementar el hipervisor), un grupo de host y un perfil de host extraídos de SCVMM, y drivers para LC Drivers Injection.

**ⓘ | NOTA:** Los perfiles de hipervisor se aplican solo a la extensión de la consola de OMIMSSC para SCVMM.

## Creación de perfil de hipervisor

Puede crear un perfil del hipervisor y utilizarlo para implementar el sistema operativo en los servidores.

#### Prerrequisitos

- Durante la creación de perfiles del hipervisor, se crea la ISO de WinPE necesaria y está disponible en la carpeta de recurso compartido de OMIMSSC IG. Para actualizar la imagen de WinPE, consulte [Actualización de WinPE](#).
- En SCVMM, cree un grupo de hosts, un perfil de host o un perfil de computadora física.

#### Pasos

- 1 En OMIMSSC, lleve a cabo cualquiera de las siguientes tareas:
  - En el tablero de OMIMSSC, haga clic en **Create Hypervisor Profiles (Crear perfiles del hipervisor)**.
  - En el panel de navegación de la izquierda, haga clic en **Profiles (Perfiles) > Hypervisor Profiles (Perfiles del hipervisor) > Create (Crear)**.
- 2 Haga clic en **Hypervisor Profile Wizard (Asistente de perfiles del hipervisor) > Welcome (Bienvenida) > Next (Siguiente)**.
- 3 En **Hypervisor Profile (Perfil del hipervisor)**, proporcione un nombre y una descripción para el perfil, y haga clic en **Next (Siguiente)**.
- 4 En la página de información de **SCVMM**:
  - a Para **SCVMM Host Group Destination (Destino de grupo de hosts de SCVMM)**, seleccione un grupo de hosts de SCVMM en el menú desplegable para agregar el host en este grupo.

- b Desde **SCVMM Host Profile/Physical Computer Profile (Perfil de host/perfil de computadora física de SCVMM)**, seleccione un perfil de host o un perfil de computadora física de SCVMM que incluya información de configuración que se aplicará en los servidores.
- 5 En **WinPE Boot Image Source (Origen de imagen de arranque de WinPE)**:
  - a Seleccione el método que desea utilizar para acceder al sistema operativo y los valores asociados y, en **Network WinPE ISO Name (Nombre de ISO de WinPE de red)**,
  - b seleccione la ISO del sistema operativo que desea utilizar y haga clic en **Next (Siguiendo)**.
- 6 (Opcional) Para habilitar LC driver injection:
  - a Seleccione el sistema operativo que desea implementar de modo que se escojan los controladores correspondientes
  - b Seleccione **Enable LC Drivers Injection (Habilitar LC Drivers Injection)**
  - c Seleccione la versión del hipervisor en **Hypervisor Version (Versión del hipervisor)**.
- 7 En **Summary (Resumen)**, haga clic en **Finish (Terminar)**.

## Modificación de un perfil de hipervisor

### Acerca de esta tarea

Tenga en cuenta lo siguiente al modificar un perfil de hipervisor:

- Puede modificar el perfil del host, el grupo de hosts y los controladores de Lifecycle Controller.
- Puede cambiar el nombre de ISO de WinPE. Sin embargo, no podrá modificar la imagen ISO.

### Pasos

- 1 Seleccione el perfil que desea modificar y haga clic en **Edit (Editar)**.
- 2 Proporcione los detalles y haga clic en **Finish (Finalizar)**.

## Eliminación de perfil de hipervisor

Seleccione el perfil que desea eliminar y haga clic en **Delete (Eliminar)**.

# Inicio de la configuración e implementación

En la página **Configuration and Deployment (Configuración e implementación)**, aparece una lista de todos los servidores host y sin asignar. Mediante el nombre de host o la dirección IP de un servidor, puede ver los detalles del servidor, como la dirección IP de la iDRAC o el nombre de host, el identificador del servidor, el FQDN del clúster, la etiqueta de servicio del chasis, el modelo de servidor, la generación del servidor, la CPU, la memoria y el estado de cumplimiento. Si coloca el ratón sobre la columna **Hardware Compatibility (Compatibilidad de hardware)**, puede ver las versiones del BIOS, la iDRAC, el LC y los paquetes de controladores.

## Acerca de esta tarea

Antes de iniciar las extensiones de la consola de OMIMSSC, compruebe la configuración del modo de bloqueo del sistema iDRAC. La configuración del modo de bloqueo del sistema está disponible en la iDRAC para la 14.ª generación de servidores PowerEdge. Si este ajuste está activado, se bloquea la configuración del sistema, incluidas las actualizaciones de firmware. Una vez que está habilitado el modo de bloqueo del sistema, los usuarios no pueden cambiar los valores de configuración. Esta configuración está diseñada para proteger el sistema de cambios accidentales. El estado del modo de bloqueo del sistema se representa con una imagen de un candado junto a la dirección IP de la iDRAC del servidor.

- Aparece la imagen de un candado junto con la dirección IP de la iDRAC del servidor si el ajuste está habilitado en ese sistema.
- Aparece la imagen de un candado abierto junto con la dirección IP de la iDRAC del servidor si el ajuste está deshabilitado en ese sistema.

Para obtener más información sobre el modo de bloqueo del sistema iDRAC, consulte los documentos sobre la iDRAC disponibles en [dell.com/support](http://dell.com/support):

**ⓘ NOTA:** Para la 14.ª generación de servidores PowerEdge, asegúrese de deshabilitar manualmente el modo de bloqueo del sistema de los hosts administrados desde la consola de la iDRAC.

En la página **Configuration and Deployment (Configuración e implementación)**, realice las siguientes tareas:

- [Descubrir servidores](#)
- Actualice la página para ver información actualizada
- [Eliminar servidores de OMIMSSC](#)
- [Sincronizar con MSSC inscritos](#)
- [Resolver errores de sincronización](#)
- [Asignar la Plantilla operativa y ejecutar el Plantilla operativa operativa](#)
- [Implementar la Plantilla operativa](#)
- Correlacionar servidores host con grupos de clúster y el chasis al que pertenece el servidor
- [Iniciar consola de la iDRAC](#)

**ⓘ NOTA:** Si el servidor no forma parte de un chasis, el campo Chassis Service Tag (Etiqueta de servicio del chasis) aparece en blanco.

**ⓘ NOTA:** Si el servidor host es parte de un clúster, para correlacionar un servidor con su grupo de clúster y para conocer la información del chasis, consulte las columnas Cluster FQDN (FQDN del clúster) y Chassis Service Tag (Etiqueta de servicio del chasis).

**ⓘ NOTA:** Para trabajar con los servidores detectados en versiones anteriores del dispositivo OMIMSSC, vuelva a detectar los servidores.

**ⓘ NOTA:** Si inicia sesión en OMIMSSC como administrador delegado, puede ver todos los servidores host y servidores sin asignar que no sean específicos de este usuario. Por lo tanto, asegúrese de que tiene los privilegios necesarios antes de realizar cualquier operación en los servidores.

- ① **NOTA:** Si el servidor cumple con la Plantilla operativa, aparecerá un cuadro de color verde con una marca de verificación junto a la Plantilla operativa asignada.
- ① **NOTA:** Si el servidor no cumple con la Plantilla operativa, aparecerá un mensaje de advertencia de color rojo junto a la Plantilla operativa asignada.

Para ver los servidores:

#### **Paso**

En la consola de OMIMSSC, haga clic en **Configuration and deployment (Configuración e implementación)**.

- ① **NOTA:** Todos los grupos de servidores que existen en el MSSC registrado aparecen en OMIMSSC, ya que esta página no es específica de ningún usuario. Asegúrese de que tiene acceso para realizar cualquier operación en esos servidores.

Todos los servidores detectados o sincronizados con el MSSC registrado aparecen en las fichas **Unassigned Servers (Servidores sin asignar)** o **Hosts**.

# Detección de servidores y sincronización con la consola de MSSC

La detección es el proceso de añadir servidores PowerEdge sin sistema operativo o servidores host compatibles en OMIMSSC, y la sincronización con la consola de MSSC le permite agregar servidores host de la consola de SCCM o SCVMM en OMIMSSC.

Temas:

- [Acerca de la configuración del servidor de referencia](#)
- [Detección de servidores en OMIMSSC](#)
- [Detección de servidores en la extensión de la consola de OMIMSSC para SCCM](#)
- [Detección de servidores en la extensión de la consola de OMIMSSC para SCVMM](#)
- [Requisitos del sistema para los sistemas administrados](#)
- [Descubrimiento de servidores mediante descubrimiento automático](#)
- [Detección manual de servidores](#)
- [Sincronización de las extensiones de la consola de OMIMSSC con el SCCM inscrito](#)
- [Sincronización de la extensión de la consola de OMIMSSC con el SCVMM inscrito](#)
- [Sincronización con MSSC inscrito](#)
- [Resolución de errores de sincronización](#)
- [Eliminación de servidores de OMIMSSC](#)
- [Inicio de la consola de la iDRAC](#)

## Acerca de la configuración del servidor de referencia

Una configuración del servidor de referencia es una configuración de servidor con una secuencia de arranque preferida, BIOS, configuraciones de RAID, configuración de hardware, atributos de actualización de firmware y parámetros del sistema operativo que se ajusta perfectamente a una organización.

Detecte un servidor de referencia capturando estos valores en una Plantilla operativa y replicándola entre diferentes servidores con la misma configuración de hardware.

## Detección de servidores en OMIMSSC

Puede detectar hosts y servidores sin asignar en OMIMSSC. La información sobre los servidores detectados se guarda en la base de datos de OMIMSSC.

Tenga en cuenta los siguientes puntos tras detectar un servidor:

- El servidor detectado se agrega a la ficha **Hosts** o **Unassigned (Sin asignar)** en la página **Configuration and Deployment (Configuración e implementación)** de OMIMSSC.
- El servidor detectado se marca como compatible con el hardware cuando contiene las versiones admitidas del firmware de LC, iDRAC y BIOS para funcionar con OMIMSSC. Para obtener información acerca de las versiones compatibles, consulte las *Notas de la versión de OpenManage Integration para Microsoft System Center*.

- Una licencia se consume tras detectar un servidor.  
El recuento de **Licensed Nodes (Nodos con licencia)** en la página **License Center** disminuye a medida que se detectan servidores.
- Cuando se detecta un servidor PowerEdge con un sistema operativo implementado y dicho servidor ya está presente en la consola de SCCM o SCVMM, el servidor figurará como un servidor host en la ficha **Hosts** en las extensiones de la consola de OMIMSSC donde se inició la detección.
  - Si el host es un servidor modular, la etiqueta de servicio del chasis que contiene el servidor también aparece en la página **Configuration and Deployment (Configuración e implementación)**.
- Cuando detecta un servidor PowerEdge que no figura en SCCM o SCVMM, dicho servidor aparecerá como un servidor sin asignar en la ficha **Unassigned (Sin asignar)** en todas las extensiones de la consola de OMIMSSC inscritas.

Puede detectar servidores Dell EMC mediante sus direcciones IP de la iDRAC usando lo siguiente:

- [Descubrimiento automático](#)
- [Detección manual](#)

## Detección de servidores en la extensión de la consola de OMIMSSC para SCCM

Tras detectar un servidor, este se agrega a uno de los siguientes grupos o colecciones predefinidos de SCCM: **All Lifecycle Controller Servers collection (Colección de todos los servidores de LifeCycle Controller)** e **Import Dell Server collection (Colección de servidores Dell de importación)** que se crean en **Device Collections (Colecciones de dispositivos)**.

Si el servidor detectado no está presente en SCCM, o si no hay grupos o colecciones predefinidos en SCCM, se crean las colecciones predefinidas y los servidores detectados se agregan al grupo correspondiente.

**NOTA:** El servidor detectado se marca como compatible con el hardware cuando contiene las versiones admitidas del firmware de LC, iDRAC y BIOS necesarias para funcionar con OMIMSSC. Para obtener más información acerca de las versiones compatibles, consulte las *Notas de la versión de OpenManage Integration para Microsoft System Center*.

## Detección de servidores en la extensión de la consola de OMIMSSC para SCVMM

Puede detectar los hosts de Hyper-V, los hosts de Hyper-V modulares y los servidores sin asignar en la extensión de la consola de OMIMSSC para SCVMM.

**NOTA:** Si el host forma parte de un clúster, se muestra el nombre de dominio completo (FQDN) del clúster.

## Requisitos del sistema para los sistemas administrados

Los sistemas administrados son los sistemas que se administran con OMIMSSC. Para detectar servidores mediante la extensión de la consola de OMIMSSC para SCCM o la extensión de la consola de OMIMSSC para SCVMM, estos son los requisitos del sistema:

- La extensión de la consola de OMIMSSC para SCVMM admite modelos de servidores modulares y monolíticos en la 11.ª generación y en generaciones posteriores de servidores PowerEdge.
- La extensión de la consola de OMIMSSC para SCCM admite modelos de servidores modulares, monolíticos y de servidores en torre en la 11.ª generación y en generaciones posteriores de servidores PowerEdge.
- Para la configuración de origen y de destino, utilice el mismo tipo de discos, es decir, solamente unidades de estado sólido (SSD), SAS o solamente unidades ATA en serie (SATA).
- Para clonar el RAID del perfil de hardware correctamente en los discos del sistema de destino, utilice discos de igual o mayor tamaño y la misma cantidad de discos que están presentes en el origen.
- No se admiten los discos virtuales segmentados RAID.
- No se admite iDRAC con LOM compartida.
- No se admite RAID configurado en la controladora externa.

- Habilite la propiedad Recopilar el inventario del sistema al iniciar (CSIOR) en sistemas administrados. Para obtener más información, consulte la documentación de iDRAC.

## Descubrimiento de servidores mediante descubrimiento automático

Para detectar automáticamente los servidores, conecte los servidores PowerEdge a la red y encienda los servidores para OMIMSSC. OMIMSSC detectará automáticamente los servidores Dell EMC sin asignar mediante la función de habilitación remota de la iDRAC. OMIMSSC funciona como el servidor de aprovisionamiento y utiliza la referencia de la iDRAC para detectar servidores Dell EMC automáticamente.

- 1 En OMIMSSC, cree un perfil de credenciales de tipo de dispositivo para los servidores Dell EMC (especificando las credenciales de la iDRAC y marcándolo como predeterminado). Para obtener más información, consulte [Creación de un perfil de credenciales](#).
- 2 Para detectar automáticamente servidores Dell EMC, realice las siguientes tareas:
  - a Deshabilite la cuenta de administrador existente en la iDRAC.

**NOTA:** Se recomienda tener una cuenta de usuario invitado con privilegios de operador para iniciar sesión en la iDRAC por si ocurre un error en la detección automática.

- b Para habilitar la detección automática del servidor de destino, ingrese en **iDRAC Settings (Configuración de la iDRAC)** y en **Remote Enablement (Habilitación remota)**, y seleccione la opción **Enabled (Habilitado)** para la función **Enable Auto-Discovery (Habilitar detección automática)**.
- c Después de activar la detección automática, proporcione la dirección IP del servidor de aprovisionamiento (la dirección IP del servidor donde OMIMSSC está instalado) y reinicie el servidor.

## Detección manual de servidores

Puede detectar manualmente los servidores PowerEdge mediante una dirección IP o un intervalo IP. Para detectar servidores, proporcione la dirección IP de la iDRAC y las credenciales de tipo de dispositivo de un servidor. Cuando detecte servidores usando un intervalo IP, especifique un intervalo IP (IPv4) (dentro de una subred). Para hacerlo, incluya el intervalo inicial y uno final.

- 1 En la consola de OMIMSSC, realice una de las acciones siguientes:
  - En el escritorio, haga clic en **Discover Unassigned Servers (Descubrir servidores sin asignar)**.
  - En el panel de navegación, haga clic en **Configuration and Deployment (Configuración e implementación)** y haga clic en **Discover (Detectar)**.
- 2 En la página **Discover (Detectar)**, seleccione la opción requerida:
  - **Discover Using an IP Address (Detectar mediante una dirección IP)**. Esta opción permite detectar un servidor mediante una dirección IP.
  - **Discover Using an IP Range (Detectar mediante un intervalo IP)**. Esta opción permite detectar todos los servidores dentro de un intervalo IP.
- 3 Seleccione el perfil de credenciales de tipo de dispositivo o haga clic en **Create New (Crear nuevo)** para crear un perfil de credenciales de tipo de dispositivo.

El perfil seleccionado se aplica a todos los servidores.
- 4 En **Dell iDRAC IP address (Dirección IP de la iDRAC de Dell)**, proporcione la dirección IP del servidor que desea detectar.
- 5 En **Discover Using an IP Address or IP Address Range (Detectar mediante una dirección IP o un rango de direcciones IP)**, realice alguna de las acciones siguientes:
  - En **IP Address Start Range (Intervalo inicial de dirección IP)** y **IP Address End Range (Intervalo final de dirección IP)**, proporcione el intervalo de direcciones IP que desee incluir, es decir, los intervalos inicial y final.
  - Seleccione **Enable Exclude Range (Habilitar intervalo de exclusión)** si desea excluir un intervalo de direcciones IP. En **IP Address Start Range (Intervalo inicial de dirección IP)** y **IP Address End Range (Intervalo final de dirección IP)**, proporcione el intervalo que desee excluir.
- 6 Introduzca un nombre de trabajo exclusivo y haga clic en **Finish (Finalizar)**.
- 7 (Opcional) Para realizar un seguimiento de este trabajo, seleccione la opción **Go to the Job List (Ir a la lista de trabajos)**. Aparecerá la página **Jobs and Logs Center (Centro de trabajos y registros)**. Expanda el trabajo de detección para ver el progreso del trabajo en la ficha **Running (En ejecución)**.

# Sincronización de las extensiones de la consola de OMIMSSC con el SCCM inscrito

Puede sincronizar todos los servidores PowerEdge (host y sin asignar) de SCCM para OMIMSSC.

## Prerrequisitos

Antes de sincronizar los servidores PowerEdge con la extensión de la consola de OMIMSSC y la consola del SCCM o SCVMM inscrito, asegúrese de que se cumplan los siguientes requisitos:

- Se necesitan los datos del perfil de credenciales predeterminado de la iDRAC de los servidores.
- Actualice **Dell Default Collection (Colección predeterminada de Dell)** antes de sincronizar OMIMSSC con SCCM. Sin embargo, si se detecta un servidor sin asignar en SCCM, se agregará a **Import Dell server collection (Importar la colección de servidores Dell)**. Para agregar este servidor a **Dell Default Collection (Colección predeterminada de Dell)**, agregue la dirección IP de la iDRAC del servidor en la página OOB.

## Acerca de esta tarea

Después de sincronizar OMIMSSC con SCCM, si el servidor no está en SCCM, se crearán las colecciones **All Dell Lifecycle Controller Servers (Todos los servidores de Dell LifeCycle Controller)** e **Import Dell server (Importar servidor Dell)** en **Device Collections (Colecciones de dispositivos)** y el servidor se agregará al grupo correspondiente.

# Sincronización de la extensión de la consola de OMIMSSC con el SCVMM inscrito

Puede sincronizar todos los hosts Hyper-V de Dell EMC, los clústeres de host Hyper-V, los hosts Hyper-V modulares y los servidores sin asignar de las consolas de SCVMM con la extensión de la consola de OMIMSSC para SCVMM. Además, obtendrá la información de inventario del firmware más reciente de los servidores tras la sincronización.

Tenga en cuenta los siguientes puntos antes de sincronizar OMIMSSC con SCVMM:

- La sincronización utiliza los detalles del perfil de credenciales del iDRAC predeterminados de los servidores.
- Si Baseboard Management Controller (BMC) en el servidor host no está configurada con la dirección IP de la iDRAC, no podrá sincronizar el servidor host con OMIMSSC. Por lo tanto, configure la BMC en SCVMM (para obtener más información, consulte el artículo de MSDN en [technet.microsoft.com](http://technet.microsoft.com)) y, a continuación, sincronice OMIMSSC con SCVMM.
- SCVMM R2 admite varios hosts en el entorno y, por este motivo, la sincronización es una tarea de ejecución larga. La sincronización se efectúa de la siguiente manera:
  - Los hosts que se enumeran en el entorno de SCVMM se agregan a la ficha **Hosts** del dispositivo OMIMSSC.
  - Si el servidor aparece como un servidor sin asignar y se agrega manualmente a SCVMM, el servidor se agregará a la ficha **hosts** del dispositivo OMIMSSC después de la sincronización.
  - Si un servidor host pertenece a un clúster Hyper-V, los detalles del clúster estarán disponibles en la ficha **Hosts**. El servidor host se agregará o se trasladará al grupo de actualización del clúster y podrá ver esta información en la página **Maintenance Center (Centro de mantenimiento)**.
  - Si un host es un servidor modular, la etiqueta de servicio del chasis que contiene el servidor modular también se agregará a la ficha **Hosts**. Si el servidor modular no pertenece a un clúster Hyper-V, el servidor host se agregará o se trasladará al grupo de actualización del chasis y podrá ver esta información en la página **Maintenance Center (Centro de mantenimiento)**.
  - Los cambios que se realicen en los detalles del inventario de host, como nombre de host, dirección IP de la iDRAC, memoria, pertenencia al clúster, etc., se actualizan en la ficha **Hosts**.
  - Si se proporciona un origen de actualizaciones predeterminado, el inventario de firmware se compara con el origen de actualizaciones y la información más reciente se agrega al grupo de actualización.

# Sincronización con MSSC inscrito

En OMIMSSC, haga clic en **Configuration and Deployment (Configuración e implementación)** y, luego, haga clic en **Synchronize with OMIMSSC (Sincronizar con OMIMSSC)** para sincronizar todos los hosts que se enumeran en el MSSC inscrito con el dispositivo OMIMSSC.

## Resolución de errores de sincronización

Los servidores que no están sincronizados con OMIMSSC aparecen con su dirección IP de la iDRAC y el nombre del host.

### Acerca de esta tarea

- ① **NOTA:** Para todos los servidores que no están sincronizados debido a problemas (por ejemplo, credenciales o dirección IP de la iDRAC no válidas, o problemas de conectividad u otros inconvenientes), es necesario resolver estas situaciones antes de la sincronización.
- ① **NOTA:** Durante la resincronización, los servidores host eliminados del entorno de MSSC inscrito se trasladan a la ficha **Unassigned Servers (Servidores sin asignar)** en las extensiones de la consola de OMIMSSC. Si se retira un servidor, elimínelo de la lista de servidores sin asignar.

Para resincronizar los servidores con problemas en el perfil de credenciales, haga lo siguiente:

### Pasos

- 1 En OMIMSSC, haga clic en **Configuration and Deployment (Configuración e implementación)** y, luego, haga clic en **Resolve Sync Errors (Resolver errores de sincronización)**.
- 2 Seleccione los servidores para resincronizar y, luego, seleccione el perfil de credenciales; o bien, para crear un perfil de credenciales, haga clic en **Create New (Crear nuevo)**.
- 3 (Opcional) Proporcione un nombre de trabajo y, si es necesario, seleccione la opción **Go to the Job List (Ir a la lista de trabajos)** para ver el estado del trabajo automáticamente una vez que se envíe.
- 4 Haga clic en **Finish (Finalizar)** para enviar el trabajo.

## Eliminación de servidores de OMIMSSC

### Acerca de esta tarea

Después de eliminar un servidor, se libera la licencia consumida.

Puede eliminar un servidor de la lista en OMIMSSC según los siguientes criterios:

- Un servidor sin asignar que aparece en la ficha **Unassigned servers (Servidores sin asignar)**.
- Si se elimina un servidor host que se aprovisiona en SCCM o SCVMM inscritos y que está en OMIMSSC en la ficha **Hosts**, primero elimine el servidor en SCCM o SCVMM y, luego, elimine el servidor de OMIMSSC.

### Pasos

- 1 En la consola de OMIMSSC, haga clic en **Configuration and deployment (Configuración e implementación)**:
  - Para eliminar servidores sin asignar, en la ficha **Unassigned Servers (Servidores sin asignar)**, seleccione el servidor y haga clic en **Delete (Eliminar)**.
  - Para eliminar servidores host, en la ficha **Host Servers (Servidores host)**, seleccione el servidor y haga clic en **Delete (Eliminar)**.
- 2 En el cuadro de diálogo de confirmación, haga clic en **Yes (Sí)**.

# Inicio de la consola de la iDRAC

En **Configuration and Deployment (Configuración e implementación)**, en las fichas **Unassigned Servers (Servidores sin asignar)** o **Hosts**, haga clic en la dirección **iDRAC IP (IP de iDRAC)** del servidor.

**NOTA:** Si utiliza el sistema operativo Windows 2012 y iDRAC versión 2.40.40.40 o una versión de firmware posterior, habilite la compatibilidad con TLS 1.1 y posterior según el explorador web para iniciar la consola de iDRAC.

# Licencias de OMIMSSC

OMIMSSC tiene dos tipos de licencias:

- Licencia de evaluación: Esta es una versión de prueba de la licencia que contiene una licencia de evaluación para cinco servidores (hosts o sin asignar) y que se importa automáticamente después de la instalación. Se aplica solamente a servidores de la 11.ª generación y generaciones posteriores de los servidores Dell EMC.
- Licencia de producción: Puede adquirir la licencia de producción de Dell EMC para la cantidad de servidores que OMIMSSC administrará. Esta licencia incluye soporte para el producto y actualizaciones del dispositivo OMIMSSC.

Cuando adquiere una licencia, el archivo .XML (clave de licencia) está disponible para descargarlo en la Tienda Digital de Dell. Si no puede descargar su(s) clave(s) de licencia, póngase en contacto con el soporte de Dell en [www.dell.com/support/softwarecontacts](http://www.dell.com/support/softwarecontacts) para encontrar el número de teléfono del soporte regional de Dell para su producto.

Puede detectar servidores en OMIMSSC con un solo archivo de licencia. Si se detecta un servidor en OMIMSSC, se utiliza una licencia. Si se elimina un servidor, una licencia se libera. Se creará una entrada en el registro de actividades de OMIMSSC en los siguientes casos:

- Cuando se importa un archivo de licencia
- Cuando se elimina un servidor de OMIMSSC y se libera una licencia
- Cuando se usa una licencia después de detectar un servidor

Después de realizar una actualización de una licencia de evaluación a una de producción, la licencia de evaluación se sobrescribirá con la licencia de producción. El recuento de **License Nodos (Nodos de la licencia)** es igual a la cantidad de licencias de producción adquirida.

Temas:

- [Opciones después de cargar las licencias](#)
- [Cumplimiento](#)
- [Importación de licencias en OMIMSSC](#)
- [Visualización de información detallada de licencias](#)

## Opciones después de cargar las licencias

A continuación, se muestran las opciones admitidas para función de licencias en OMIMSSC.

### Archivo de licencia para adquisiciones nuevas

Cuando realiza un pedido para adquirir una nueva licencia, Dell le envía un mensaje de correo electrónico sobre la confirmación del pedido, y usted puede descargar el nuevo archivo de licencia desde la Tienda Digital de Dell. La licencia está en formato .xml. Si la licencia está en formato .zip, extraiga el archivo de licencia .xml desde el archivo .zip antes de cargarla.

## Licencias de apilamiento

Puede apilar varias licencias de producción para aumentar la cantidad de servidores admitidos a la suma de los servidores en las licencias cargadas. No es posible apilar una licencia de evaluación. La cantidad de servidores admitidos no se podrá aumentar mediante apilamiento y será necesario el uso de varios dispositivos.

Si ya hay varias licencias cargadas, la cantidad de servidores admitidos se compone de la suma de los servidores en las licencias en el momento en que se cargó la última licencia.

## Reemplazo de licencias

Si hay un problema con su pedido, o si intenta cargar un archivo modificado o dañado, aparecerá un mensaje de error. Puede solicitar otro archivo de licencia en la Tienda Digital de Dell. Una vez que reciba la licencia de reemplazo, esta contendrá los mismos Id. de autorización que la licencia anterior. Cuando cargue una licencia de reemplazo, esta reemplazará a la licencia actual que ya se haya cargado con el mismo Id. de autorización.

## Reimportación de licencias

Si intenta importar el mismo archivo de licencia, aparecerá un mensaje de error. Debe adquirir una licencia nueva e importarla.

## Importación de varias licencias

Puede importar varios archivos de licencia con diferentes Id. de autorización para aumentar la cantidad de servidores detectados y conservados en OMIMSSC.

## Cumplimiento

### Actualización de licencias

Se le permitirá trabajar con OMIMSSC con el archivo de licencia actual para todas las generaciones de servidores admitidas. Si el archivo de licencia no es compatible con la generación más reciente del servidor, debe adquirir nuevas licencias.

### Licencia de evaluación

Cuando vence una licencia de evaluación, muchas áreas clave dejan de funcionar y aparece un mensaje de error.

## Consumo de licencias en OMIMSSC después de la detección de servidores

Cuando intente agregar un host o detectar un servidor sin sistema operativo, se le avisará acerca del uso y se le recomendará adquirir nuevas licencias en los siguientes casos:

- Si la cantidad de servidores con licencia supera la cantidad de licencias adquiridas.
- Si los servidores detectados equivalen a la cantidad de licencias adquiridas.
- Si supera la cantidad de licencias adquiridas, se le otorgará una licencia de cortesía.
- Si supera la cantidad de licencias adquiridas y todas las licencias de cortesía.

**NOTA:** Las licencias de cortesía equivalen al 20 % de la cantidad total de licencias adquirida. Por lo tanto, la cantidad real de licencias que puede utilizar en OMIMSSC es igual al total de licencias adquiridas más las licencias de cortesía.

## Importación de licencias en OMIMSSC

### Acerca de esta tarea

Después de adquirir una licencia, impórtela en OMIMSSC. Para ello, siga estos pasos:

### Pasos

- 1 En el Portal para administradores, haga clic en **License Center (Centro de licencias)**.
- 2 Haga clic en **Import License** y examine para seleccionar el archivo de licencia descargado desde la Tienda Digital de Dell.

**NOTA:** Solo puede importar archivos de licencia válidos. Si el archivo está dañado o fue manipulado, aparecerá un mensaje de error según corresponda. Descargue el archivo nuevamente desde la Tienda Digital de Dell o póngase en contacto con un representante de Dell para obtener un archivo de licencia válido.

## Visualización de información detallada de licencias

- 1 Abra un navegador y proporcione la URL del dispositivo OMIMSSC.  
Aparecerá la página de inicio de sesión del Portal para administradores de OMIMSSC.
- 2 Haga clic en **License Center (Centro de licencias)**.  
En la página, figura la siguiente información:

**License Summary (Resumen de licencia):** Información detallada de la licencia para OMIMSSC.

- **Licensed nodes (Nodos con licencia):** Cantidad total de licencias adquiridas.
- **Nodes in use (Nodos en uso):** Cantidad de servidores detectados y que han consumido la licencia.
- **Nodes available (Nodos disponibles):** Nodos de licencia restantes que es posible detectar en OMIMSSC.

**Managing Licenses (Administración de licencias):** Aquí es posible ver cada archivo de licencia importado junto con la información detallada, como el Id. de autorización, la descripción del producto, la fecha en que el archivo de licencia se importó, la fecha desde que el archivo de licencia es válido y la lista de todas las generaciones de servidores compatibles con la licencia.

## Plantilla operativa

La Plantilla operativa implementa sistemas operativos y actualiza versiones de firmware de los servidores PowerEdge en entornos MSSC. Puede capturar toda la configuración del servidor desde un servidor de referencia y, luego, ajustar las configuraciones de hardware, establecer los parámetros del sistema operativo y los atributos de actualización de firmware en una plantilla operativa e implementar esta plantilla en varios servidores. También puede comprobar el estado de cumplimiento del servidor con una plantilla operativa asignada y ver las diferencias en una página de resumen. Para obtener más información sobre el servidor de referencia, consulte [Acerca de la configuración del servidor de referencia](#).

En la siguiente tabla, figuran todas las funciones que admite la plantilla operativa:

**Tabla 4. Funcionalidad de OMIMSSC**

Componente	Configuración e implementación	Actualización del firmware	Ver el inventario	Estado de cumplimiento de plantilla operativa
BIOS	Sí	Sí	Sí	Sí
iDRAC	Sí	Sí	Sí	Sí
NIC/CNA	Sí	Sí	Sí	Sí
RAID	Sí	Sí	Sí	Sí
FC	Sí	Sí	Sí	Sí
Windows	<b>Sí</b>	—	No	—
RHEL	<b>Sí</b>	—	No	—
ESXI	<b>Sí</b>	—	No	—

Tenga en cuenta los siguientes puntos antes de implementar una Plantilla operativa:

- Si selecciona cualquiera de los componentes de hardware de configuración (BIOS, RAID NIC/CNA, FC o iDRAC), asegúrese de seleccionar los servidores del mismo modelo.
- Si selecciona los componentes de firmware, puede actualizar el firmware en todos los servidores.

Temas:

- [Preparación para la implementación](#)
- [Administración de Plantilla operativa](#)

## Preparación para la implementación

Antes de implementar una Plantilla operativa, cree una imagen WinPE, una secuencia de tareas y una Plantilla operativa.

### Creación de imagen ISO de WinPE

Se asigna un nombre de trabajo exclusivo a cada actualización del entorno de preinstalación de Windows (WinPE). Se necesita un servidor de entorno previo a la ejecución (PXE) para crear una imagen ISO de WinPE. La ISO de WinPE se crea a partir de la imagen de WinPE y

Dell OpenManage Deployment Toolkit (DTK). Una vez que se crea una imagen ISO de WinPE, detenga el servidor PXE. Asegúrese de que estén instalados en LifeCycle Controller los paquetes de drivers relacionados con el sistema operativo correspondiente. Mientras se utiliza la versión más reciente de DTK para crear una imagen ISO de WinPE, utilice la versión de WinPE de los archivos de DTK. El archivo de DTK contiene las versiones de firmware necesarias para los servidores en los que implementará los sistemas operativos.

### Prerequisito

**NOTA:** Mientras se utiliza la versión más reciente de DTK para crear una imagen ISO de WinPE, utilice el archivo de Dell OpenManage Deployment Toolkit para Windows. El archivo de Dell OpenManage Deployment Toolkit para Windows contiene las versiones de firmware necesarias para los sistemas en los que implementará los sistemas operativos. Use la versión más reciente del archivo y no utilice el archivo de Dell OpenManage Deployment Toolkit Windows Driver Cabinet para la actualización de WinPE.

### Pasos

- 1 Agregue el servidor PXE al dispositivo OMIMSSC.
- 2 Después de agregar el servidor PXE, copie el archivo **boot.wim** desde el servidor PXE a la carpeta WIM del recurso compartido de SCVMM de OMIMSSC IG. El archivo **boot.wim** se encuentra en la siguiente ruta de acceso: **C:\RemotelInstall\DCMgr\Boot\Windows\Images**

**NOTA:** No cambie el nombre del archivo **boot.wim**.

## Extracción de los drivers de DTK

### Acerca de esta tarea

DTK es un archivo ejecutable autoextraíble.

Para trabajar con DTK:

### Pasos

- 1 Haga doble clic en el archivo ejecutable de DTK.
- 2 Para extraer los drivers de DTK, seleccione la carpeta, por ejemplo **C:\DTK501**.
- 3 Copie la carpeta de DTK que se extrajo a la carpeta de recurso compartido de DTK de IG. Por ejemplo, **\\OMIMSSC IG Share\DTK\DTK501**.

**NOTA:** Si está actualizando de SCVMM SP1 a SCVMM R2 realice la actualización a Windows PowerShell 4.0 y cree una imagen ISO de WinPE.

## Actualización de una imagen de WinPE

- 1 En OMIMSSC, seleccione **WinPE Update (Actualización de WinPE)** en **Image Source (Origen de la imagen)**. En **Custom WinPE Image Path (Ruta de acceso a imagen de WinPE personalizada)**, proporcione la ruta de acceso de la imagen de WinPE. Por ejemplo, **\\OMIMSSC IG Share\WIM\boot.wim**.
- 2 En **DTK Path (Ruta de acceso de DTK)**, para **DTK Drivers Path (Ruta de acceso de controladores de DTK)**, proporcione la ubicación de los controladores de Dell Deployment Toolkit. Por ejemplo, **\\OMIMSSC IG Share\DTK\DTK501**.
- 3 Proporcione los archivos para uno de los siguientes:
  - Proporcione el nombre de archivo de WIM para SCCM.
  - Proporcione el nombre de archivo de ISO para SCVMM.
- 4 Para ver la lista de trabajos, seleccione **Go to the Job List (Ir a la lista de trabajos)**. Se asigna un nombre de trabajo exclusivo a cada actualización del entorno de preinstalación de Windows (WinPE).
- 5 Haga clic en **Update (Actualizar)**. En **\\OMIMSSC IG Share\ISO**, se crea la ISO de WinPE con el nombre proporcionado en el paso anterior.

# Secuencia de tareas

Esta opción se utiliza para capturar la imagen del sistema operativo o implementar un sistema operativo en la consola de SCCM. Antes de crear una Plantilla operativa, se recomienda completar los siguientes requisitos previos.

- En Configuration Manager, asegúrese de que el sistema se haya detectado y se encuentre en **Assets and Compliance (Activos y cumplimiento) > Device Collections (Colecciones de dispositivos) > All Dell Lifecycle Controller Servers (Todos los servidores de Dell LifeCycle Controller)**. Para obtener más información, consulte [Detección de servidores](#).
- Instale la versión del BIOS más reciente en el sistema.
- Instale la versión más reciente de Lifecycle Controller en el sistema.
- Instale la versión más reciente del firmware del iDRAC en el sistema.

**NOTA:** Siempre inicie la consola de Configuration Manager con privilegios de administrador.

## Creación de una secuencia de tareas

Puede crear una secuencia de tareas de dos maneras, y esta se usará para las configuraciones de servidor:

- Crear una secuencia de tareas específica para Dell mediante la plantilla de implementación de OMIMSSC.
- Crear una secuencia de tareas personalizada.

La secuencia de tareas continúa con el siguiente paso independientemente del éxito o la falla del comando.

## Creación de una secuencia de tareas específica de Dell

### Acerca de esta tarea

Para crear una secuencia de tareas específicas de Dell utilizando la opción **Server Deployment Template (Plantilla de implementación de servidor) de OMIMSSC**:

### Pasos

- 1 Inicie Configuration Manager.  
Aparecerá la pantalla de la consola de Configuration Manager.
- 2 En el panel izquierdo, seleccione **Biblioteca de software > Descripción general > Sistemas operativos > Secuencias de tareas**.
- 3 Haga clic con el botón derecho del ratón en **Task Sequences (Secuencias de tareas)** y, luego, en **OMIMSSC Server Deployment (Implementación de servidores de OMIMSSC) > Create OMIMSSC Server Deployment Template (Crear plantilla de implementación de servidores de OMIMSSC)**.  
Aparecerá el **OMIMSSC Server Deployment Task Sequence Wizard (Asistente de secuencias de tareas de implementación de servidor de OMIMSSC)**.
- 4 Introduzca el nombre de la secuencia de tareas en el campo **Nombre de la secuencia de tareas**.
- 5 Seleccione en la lista desplegable la imagen de inicio que desea usar.

**NOTA:** Se recomienda utilizar la imagen de inicio personalizada de Dell que creó.

- 6 En **Operating System Installation (Instalación del sistema operativo)**, seleccione el tipo de instalación del sistema operativo. Las opciones son:
  - **Use an OS WIM image (Usar una imagen WIM del sistema operativo)**
  - **Scripted OS install (Instalación del sistema operativo mediante una secuencia de comandos)**
- 7 Seleccione un paquete del sistema operativo en el menú desplegable **Operating system package to use (Paquete del sistema operativo por usar)**.
- 8 Si tiene un paquete con **unattend.xml**, selecciónelo del menú **Package with unattend.xml info (Paquete con información de unattend.xml)**. De lo contrario, seleccione **<do not select now> (no seleccionar ahora)**.
- 9 Haga clic en **Crear**.

Se muestra la ventana **Secuencia de tareas creada** con el nombre de la secuencia de tareas que creó.

- 10 Haga clic en **Cerrar** en el cuadro de mensaje de confirmación que aparece.

## Creación de una secuencia de tareas personalizada

- 1 Inicie Configuration Manager.  
Aparece la consola de Configuration Manager.
- 2 En el panel izquierdo, seleccione **Biblioteca de software > Descripción general > Sistemas operativos > Secuencias de tareas**.
- 3 Haga clic con el botón derecho del mouse en **Secuencias de tareas** y, después, haga clic en **Crear secuencias de tareas**.  
Aparece el **Asistente de creación de secuencias de tareas**.
- 4 Seleccione **Crear una nueva secuencia de tareas personalizada** y haga clic en **Siguiente**.
- 5 Introduzca un nombre para la secuencia de tareas en el cuadro de texto **Nombre de la secuencia de tareas**.
- 6 Busque la imagen de inicio de Dell que creó y haga clic en **Siguiente**.  
Aparece la pantalla **Confirmar la configuración**.
- 7 Revise la configuración y haga clic en **Siguiente**.
- 8 Haga clic en **Cerrar** en el cuadro de mensaje de confirmación que aparece.

## Edición de una secuencia de tareas

### Acerca de esta tarea

- ① **NOTA:** Mientras edita secuencias de tareas en SCCM 2016, los mensajes de referencia de objetos que faltan no enumeran el paquete **Setup windows and ConfigMgr (Configuración de Windows y Configuration Manager)**. Agregue el paquete y guarde la secuencia de tareas.

### Pasos

- 1 Inicie Configuration Manager.  
Aparecerá la pantalla de Configuration Manager.
  - 2 En el panel izquierdo, seleccione **Biblioteca de software > Sistemas operativos > Secuencia de tareas**.
  - 3 Haga clic con el botón derecho del mouse en la secuencia de tareas que desea editar y haga clic en **Editar**.  
Aparece la ventana **Editor de secuencias de tareas**.
  - 4 Haga clic en **Agregar > Implementación de Dell > Aplicar controladores a partir de Dell Lifecycle Controller**.  
Se carga la acción personalizada para la implementación de servidores Dell. Ahora, es posible hacer cambios en la secuencia de tareas.
- ① **NOTA:** Al editar una secuencia de tareas por primera vez, aparece el mensaje de error **Setup Windows and Configuration Manager (Configurar Windows y Configuration Manager)**. Para solucionarlo, cree y seleccione el paquete de actualización del cliente de Configuration Manager. Para obtener más información acerca de la creación de paquetes, consulte la documentación de Configuration Manager en [technet.microsoft.com](http://technet.microsoft.com).

## Creación de medios de arranque de Lifecycle Controller

### Acerca de esta tarea

Use esta función para crear un medio de arranque de implementación sin intervención a partir de una secuencia de tareas.

- ① **NOTA:** Esta función se aplica solo a la extensión de la consola de OMIMSSC para SCCM.

### Pasos

- 1 Inicie OMIMSSC y haga clic en **Boot Media Creation (Creación de medio de arranque)**.
- 2 En **Image Source (Origen de imagen)**, proporcione el archivo ISO que contiene la imagen del sistema operativo.  
Para obtener más información, consulte [Creación de una ISO de arranque mediante la secuencia de tareas](#).
- 3 En **Output File (Archivo de salida)**, escriba el nombre del archivo ISO, que es un archivo ISO desatendido.

- (Opcional) Para ir a la página **Jobs and logs (Trabajos y registros)** después de que haya comenzado el trabajo, seleccione la casilla de verificación **Go to the Job List (Ir a la lista de trabajos)**.
- Haga clic en **Update (Actualizar)** para guardar el archivo de salida en el recurso compartido de la ISO.

## Configuración de una ubicación predeterminada de recurso compartido para el medio de inicio de Lifecycle Controller

### Acerca de esta tarea

Para establecer una ubicación predeterminada de recurso compartido para el medio de inicio de Lifecycle Controller:

### Pasos

- En Configuration Manager, seleccione **Administration (Administración) > Site Configuration (Configuración de sitios) > Sites (Sitios)**
- Haga clic con el botón derecho del ratón en **<site server name> (nombre del servidor del sitio)**, seleccione **Configure Site Components (Configurar componentes del sitio)** y, luego, seleccione **Out of Band Management (Administración fuera de banda)**. Aparecerá la ventana **Propiedades de los componentes de administración fuera de banda**.
- Haga clic en la ficha **Lifecycle Controller**.
- En **Ubicación predeterminada del recurso compartido para el medio de inicio personalizado de Lifecycle Controller**, haga clic en **Modificar** para modificar la ubicación predeterminada del recurso compartido del medio de inicio personalizado de Lifecycle Controller.
- En la ventana **Modify Share Information (Modificar información de recurso compartido)**, introduzca un nuevo nombre de recurso compartido y una nueva ruta de acceso al recurso compartido.
- Haga clic en **OK (Aceptar)**.

## Creación de una ISP de inicio de medio de secuencia de tareas

- En Configuration Manager, en **Software Library (Biblioteca de software)**, haga clic con el botón derecho del ratón en **Task Sequences (Secuencias de tareas)** y seleccione **Create Task Sequence Media (Crear medio de secuencia de tareas)**.

### NOTA:

- Asegúrese de administrar y actualizar la imagen de inicio en todos los puntos de distribución antes de iniciar este asistente.
- OMIMSSC: OMIMSSC no admite el método de medios independientes para crear secuencias de tareas.

- En **Asistente para un medio de secuencia de tareas**, seleccione **Medios de inicio** y haga clic en **Siguiente**.
- Seleccione **Conjunto de CD/DVD**, haga clic en **Examinar** y seleccione la ubicación para guardar la imagen ISO.
- Haga clic en **Next (Siguiente)**.
- Desactive la casilla de verificación **Proteger medio con una contraseña** y haga clic en **Siguiente**.
- Navegue y seleccione **PowerEdge server Deployment Boot Image (Imagen de arranque de implementación de servidor PowerEdge)**.

### NOTA: Utilice la imagen de arranque creada usando DTK solamente.

- Seleccione el punto de distribución del menú desplegable y luego seleccione la casilla de verificación **Mostrar puntos de distribución de los sitios secundarios**.
- Haga clic en **Next (Siguiente)**.  
La pantalla **Resumen** mostrará la información del medio de secuencia de tareas.
- Haga clic en **Next (Siguiente)**.  
Se muestra la barra de progreso.
- Cuando termine, cierre el asistente.

# Para trabajar con la implementación de sistemas operativos que no sean de Windows

Asegúrese de recordar los siguientes puntos para implementar sistemas operativos que no sean de Windows en los sistemas de destino:

- El archivo ISO del sistema que no es de Windows está disponible el recurso compartido del sistema de archivos de red (NFS) o el sistema de archivos de Internet común (CIFS) con acceso de lectura y escritura.
- Confirme que el disco virtual está disponible en el sistema de destino.
- Una vez que se implementa el sistema operativo de ESXi, el servidor se traslada a la colección de **Managed Lifecycle Controller (ESXi)** en SCCM.
- Después de implementar cualquier tipo de sistema operativo que no sea de Windows, los servidores se trasladan al **Default Non-Windows Host Update Group (Grupo de actualización predeterminado de hosts que no son de Windows)**.
- Se recomienda que el adaptador de red esté conectado al puerto de red del servidor en el que se implementa el sistema operativo.

## Administración de Plantilla operativa

Puede crear, editar y eliminar una Plantilla operativa en OMIMSSC.

## Creación de una Plantilla operativa

### Prerrequisitos

Antes de crear una Plantilla operativa, asegúrese de completar las siguientes tareas:

- Detecte un servidor de referencia mediante la página **Discovery (Detección)**. Para obtener más información, consulte [Detección manual de servidores](#).
- (Opcional) Cree un origen de actualizaciones. Para obtener más información, consulte [Creación de un origen de actualizaciones](#).
- (Opcional) En OMIMSSC para SCCM:
  - Cree una secuencia de tareas.  
Para obtener más información, consulte [Creación de una secuencia de tareas](#).
  - Para las implementaciones de sistemas operativos que no sean de Windows, debe tener un perfil de credenciales de tipo de dispositivo. Para obtener más información, consulte [Creación de un perfil de credenciales](#).
  - Cree un medio de arranque desatendido. Para obtener más información, consulte [Creación de un medio de arranque de LC](#).
- (Opcional) En OMIMSSC para SCVMM:
  - Cree un perfil de hipervisor: Para obtener información sobre cómo crear un perfil de hipervisor, consulte [Crear perfil de hipervisor](#).
  - Para las implementaciones de Windows, debe tener un perfil de credenciales de tipo de dispositivo. Para obtener más información, consulte [Creación de un perfil de credenciales](#).

### Acerca de esta tarea

Puede crear una Plantilla operativa capturando la configuración del servidor de referencia. Después de capturar la configuración, puede guardar la plantilla directamente, o bien, editar los atributos del origen de actualizaciones, la configuración de hardware y el componente de Windows, según sus necesidades. Ahora es posible guardar la plantilla, que puede usarse para otros servidores PowerEdge homogéneos.

### Pasos

- 1 En OMIMSSC, realice alguno de estos pasos para abrir la Plantilla operativa:
  - En el tablero de OMIMSSC, haga clic en **Create Operational Template (Crear plantilla operativa)**.
  - En el panel de navegación, haga clic en **Profiles (Perfiles) > Operational Template (Plantilla operativa)** y, luego, haga clic en **Create (Crear)**.

Aparecerá el asistente para la **plantilla operativa**.
- 2 Introduzca un nombre y una descripción para la plantilla. También proporcione la dirección IP del servidor de referencia y haga clic en **Next (Siguiente)**.

**NOTA:** Puede capturar la configuración del servidor de referencia con iDRAC 2.0 y versiones posteriores.

- 3 En **Server Components (Componentes del servidor)**, haga clic en un componente para ver los atributos disponibles y sus valores. Los componentes son los siguientes:
  - Actualización del firmware
  - Los componentes de hardware, que son el RAID, la NIC y el BIOS
  - Sistema operativo (seleccione Windows, ESXi o RHEL)
- 4 (Opcional) Edite los valores de los atributos disponibles, si es necesario.
- 5 Seleccione la casilla de verificación para cada componente, ya que solo la configuración de los componentes seleccionados se aplicará cuando la Plantilla operativa se implemente en todas las configuraciones capturadas. En el componente **Operating System (Sistema Operativo)**, siga los pasos que se indican en cualquiera de las opciones siguientes, según lo que necesite:
  - Para la implementación de sistemas operativos Windows en SCCM, consulte [Componente de Windows para la extensión de la consola de OMIMSSC para SCCM](#).
  - Para la implementación de sistemas operativos que no sean de Windows en SCVMM, consulte [Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM](#).
  - OMIMSSC
  - Para la implementación de sistemas operativos que no sean de Windows, consulte [Componente que no sea de Windows para las extensiones de la consola de OMIMSSC](#).
- 6 Para guardar el perfil, haga clic en **Finish (Finalizar)**.

## Componente del sistema operativo Windows para la extensión de la consola de OMIMSSC para SCCM

### Acerca de esta tarea

Al crear la Plantilla operativa, ejecute los siguientes pasos para componentes de Windows:

### Pasos

- 1 Seleccione una secuencia de tareas y un método de implementación.

**NOTA:** Solo las secuencias de tareas implementadas en recopilaciones aparecen en el menú desplegable.

Para obtener más información sobre las secuencias de tareas, consulte [Task sequence \(Secuencia de tareas\)](#).

- 2 Seleccione una de las siguientes opciones para **Deployment Method (Método de implementación)**:
  - **Boot to network ISO (Iniciar en ISO de red)**. Con esta opción, se reinicia la ISO especificada.
  - **Stage ISO to vFlash and Reboot (Copiar ISO en vFlash y reiniciar)**. Con esta opción, se descarga la ISO en vFlash y se realiza el reinicio.
  - **Reboot to vFlash (Reiniciar en vFlash)**. Con esta opción, se reinicia en vFlash. Asegúrese de que la imagen ISO esté presente en vFlash.

**NOTA:** Para utilizar la opción **Reboot to vFlash (Reiniciar en vFlash)**, el nombre de la etiqueta de la partición creada en vFlash debe ser ISOIMG.

- 3 (Opcional) Para usar la imagen presente en el recurso compartido de red si la imagen presente en vFlash está dañada, seleccione la opción **Use Network ISO as Fallback (Usar ISO de red como reserva)**.
- 4 Proporcione un archivo de imagen de arranque de LC y (opcional) utilice **Enable LC Drivers Injection (Habilitar LC Drivers Injection)**. Para obtener más información sobre cómo crear una imagen de arranque de LC, consulte [Crear un medio de arranque de LC](#).
- 5 Seleccione los controladores necesarios para el sistema operativo.

# Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM

## Acerca de esta tarea

Al crear la Plantilla operativa, ejecute los siguientes pasos para componentes de Windows:

### Paso

Seleccione **Hypervisor Profile (Perfil de hipervisor)**, **Credential Profile (Perfil de credenciales)** y **Server IP from (IP del servidor de)**.

**NOTA:** Host Name (Nombre de host) y Server Management NIC (NIC de administración de servidor) son siempre valores de bloque.

Si selecciona **Server IP from (IP de servidor de)** como **Static (Estática)**, asegúrese de haber configurado la red lógica en SCVMM, y de que los siguientes valores sean valores de bloque:

- **Console Logical Network (Red lógica de consola)**
- **Subred IP**
- **Dirección IP estática**

# Componente que no sea de Windows para las extensiones de la consola de OMIMSSC

## Acerca de esta tarea

Al crear la Plantilla operativa, ejecute los siguientes pasos para componentes que no sean de Windows:

### Paso

Seleccione un sistema operativo que no sea de Windows, el tipo de carpeta de recurso compartido, el nombre de archivo ISO, la ubicación del archivo ISO y la contraseña de la cuenta root del sistema operativo.

(Opcional) Seleccione un perfil de credenciales tipo Windows para acceder al recurso compartido de CIFS.

**Host name (Nombre de host)** es un valor de bloque y, si deshabilita la opción DHCP, los siguientes campos serán valores de bloque:

- **Dirección IP**
- **Máscara de subred**
- **Default Gateway**
- **DNS primario**
- **DNS secundario**

① **NOTA:** Los tipos de recurso compartido de sistema de archivos de red (NFS) y sistema de archivos de Internet común (CIFS) se admiten para la implementación de sistemas operativos que no sean de Windows.

## Visualización de plantillas de Plantilla operativa

Para ver plantillas de Plantilla operativa, realice lo siguiente:

En la consola de OMIMSSC, haga clic en **Profiles and Templates (Perfiles y plantillas)** y, luego, haga clic en **Operational Template (Plantilla operativa)**. Todas las plantillas de Plantilla operativa aparecen aquí.

## Edición de una Plantilla operativa

### Acerca de esta tarea

Puede editar una Plantilla operativa para modificar el origen de actualizaciones, las configuraciones de hardware y los componentes del sistema operativo del servidor de referencia.

① **NOTA:** Es posible que algunos atributos dependan de otros valores de atributos. Si estos atributos no se actualizan, es posible que ocurra un error al aplicar la configuración del hardware. Por lo tanto, se recomienda no editar la configuración de referencia.

① **NOTA:** Mientras edita secuencias de tareas en SCCM 2016, los mensajes de referencia de objetos que faltan no enumeran el paquete Setup windows and ConfigMgr (Configuración de Windows y Configuration Manager). Agregue el paquete y guarde la secuencia de tareas.

### Pasos

- 1 Seleccione la plantilla que desea modificar y haga clic en **Edit (Editar)**.  
Aparecerá la página Plantilla operativa.
- 2 Edite el nombre y la descripción de la plantilla (si es necesario) y haga clic en **Next (Siguiente)**.
- 3 Para ver los atributos disponibles y sus valores en **Server Components (Componentes del servidor)**, haga clic en un componente.
- 4 Modifique los valores de los atributos disponibles si es necesario.

① **NOTA:** Seleccione la casilla de verificación para cada componente, debido a que solo las configuraciones del componente seleccionado se aplican al sistema de destino cuando se implementa la Plantilla operativa.

① **NOTA:** Independientemente de la selección realizada en la casilla de verificación para cada componente, todas las configuraciones se capturan en la plantilla.

- 5 Para el componente de sistema operativo, realice una de las siguientes tareas en función de sus necesidades:
  - Para la implementación de sistemas operativos Windows en SCCM, consulte [Componente de Windows para la extensión de la consola de OMIMSSC para SCCM](#).
  - Para la implementación de sistemas operativos que no sean de Windows en SCVMM, consulte [Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM](#).
  - Para la implementación de sistemas operativos que no sean de Windows, consulte [Componente que no sea de Windows para las extensiones de la consola de OMIMSSC](#).
- 6 Para guardar el perfil, haga clic en **Finish (Finalizar)**.

## Componente de Windows para la extensión de la consola de OMIMSSC para SCCM

Mientras edita la Plantilla operativa, siga los pasos que se mencionan en [Componente del sistema operativo Windows para las extensiones de la consola de OMIMSSC para SCCM](#).

## Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM

Mientras edita la Plantilla operativa, siga los pasos que se mencionan en [Componente del sistema operativo Windows para las extensiones de la consola de OMIMSSC para SCVMM](#).

## Componente que no sea de Windows para las extensiones de la consola de OMIMSSC

Mientras edita la Plantilla operativa, siga los pasos que se mencionan en [Componente que no sea de Windows para las extensiones de la consola de OMIMSSC](#).

## Eliminación de una Plantilla operativa

Para eliminar una Plantilla operativa, siga estos pasos.

### Acerca de esta tarea

Antes de eliminar una Plantilla operativa, asegúrese de lo siguiente:

- Que la Plantilla operativa seleccionada no esté asociada con ningún servidor. Si está asociada con un servidor, cancele la asignación y elimine la plantilla.
- Que no haya en ejecución trabajos asociados con la Plantilla operativa.

### Paso

Seleccione las plantillas que desee eliminar y haga clic en **Delete (Eliminar)**. Para confirmar, haga clic en **Yes (Sí)**.

## Plantilla operativa

Asigne una Plantilla operativa a un servidor y ejecute el cumplimiento de la Plantilla operativa. Solo después de asignar una Plantilla operativa a un servidor, podrá ver el estado de cumplimiento de la Plantilla operativa. Puede comparar la configuración de un servidor con una Plantilla operativa si le asigna la plantilla a un servidor. Una vez que asigna una Plantilla operativa, el trabajo de cumplimiento se ejecuta y el estado de la Plantilla operativa se muestra al finalizar.

- 1 En OMIMSSC, haga clic en **Configuration and Deployment (Configuración e implementación)**. Seleccione los servidores necesarios y haga clic en **Assign Operational Template and Run Compliance (Asignar la plantilla operativa y ejecutar el cumplimiento)**. Aparecerá la página **Assign Plantilla operativa and Run Compliance** (Asignar la plantilla operativa y ejecutar el cumplimiento).
- 2 Seleccione la plantilla en el menú desplegable **Plantilla operativa**, proporcione un nombre para el trabajo y, luego, haga clic en **Assign (Asignar)**.

Si el servidor cumple con la plantilla, aparecerá una marca de verificación de color **verde**.

Si el servidor no cumple con la plantilla, solo entonces podrá ver un informe resumido si hace clic en el vínculo del nombre de la plantilla, siempre y cuando los servidores no cumplan con la plantilla. La página **Plantilla operativa Compliance-Summary Report (Informe resumido de cumplimiento de la plantilla operativa)** muestra un informe resumido de las diferencias entre las configuraciones de la plantilla y del servidor.

Para ver un informe detallado, siga estos pasos:

- a Haga clic en **View Detailed Compliance (Ver cumplimiento detallado)**. Aquí figuran los componentes con valores de atributos diferentes a los de la plantilla asignada. Los colores indican los diferentes estados de cumplimiento con la Plantilla operativa.

- El amarillo indica que la configuración del servidor no coincide con los valores de la plantilla.
- El rojo indica que el componente está presente en el servidor.

## Implementación de Plantilla operativa

### Acerca de esta tarea

Puede implementar sistemas operativos Windows y que no sean Windows (ESXi y RHEL).

- NOTA:** Descargue e instale los controladores que correspondan desde [dell.com/support](http://dell.com/support) si aparece un ícono de advertencia amarillo en el Administrador de dispositivos después de implementar el sistema operativo Windows 2016 en servidores PowerEdge de 12.ª generación.

### Pasos

- 1 En OMIMSSC, haga clic en **Configuration and Deployment (Configuración e implementación)**. Seleccione los servidores en los que desea implementar una plantilla y haga clic **Deploy Plantilla operativa (Implementar plantilla operativa)**. Aparecerá la página **Deploy Plantilla operativa (Implementar plantilla operativa)**.
- 2 (Opcional) Para exportar todos los atributos marcados como valores de grupo en la plantilla seleccionada a un archivo .CSV, haga clic en **Export Pool Attributes (Exportar atributos de grupo)**. De lo contrario, vaya al paso 3.
  - NOTA:** Antes de exportar los valores de grupo, agregue al sitio de intranet local la dirección IP del servidor donde las extensiones de la consola de OMIMSSC están instaladas. Para obtener más información acerca de cómo agregar la dirección IP en el navegador Internet Explorer, consulte [Configuración del navegador](#).
  - NOTA:** Si ha exportado los valores de grupo, proporcione todos los valores para todos los atributos marcados como valores de grupo en el archivo .CSV y guarde el archivo. En Attribute Value Pool (Grupo de valores de atributo), seleccione este archivo para importarlo.
  - NOTA:** Asegúrese de seleccionar un archivo .CSV que tenga todos los atributos correspondientes y de que las credenciales o la dirección IP de la iDRAC no cambien debido a la plantilla, ya que OMIMSSC no hace un seguimiento del trabajo después de que la dirección IP y las credenciales de la iDRAC cambian, y el trabajo se marca como incompleto a pesar de que se haya completado satisfactoriamente en la iDRAC.
  - NOTA:** Descargue e instale los controladores que correspondan desde [dell.com/support](http://dell.com/support) si aparece un ícono de advertencia amarillo en el Administrador de dispositivos después de implementar el sistema operativo Windows 2016 en servidores PowerEdge de 12.ª generación.
- 3 Proporcione un nombre de trabajo exclusivo y la descripción del trabajo, y haga clic en **Deploy (Implementar)**. Para ver los trabajos, seleccione **Go to the Job List (Ir a la lista de trabajos)**.

## Cancelación de la asignación de Plantilla operativa

- 1 En OMIMSSC, haga clic en **Configuration and deployment (Configuración e implementación)**.
- 2 Seleccione los servidores en los que cancelará la asignación de la plantilla y, luego, haga clic en **Assign Plantilla operativa and Run Compliance (Asignar la plantilla operativa y ejecutar el cumplimiento)**. Aparecerá la página **Assign Plantilla operativa and Run Compliance (Asignar la plantilla operativa y ejecutar el cumplimiento)**.
- 3 Seleccione **Unassign (Cancelar asignación)** en el menú desplegable Plantilla operativa y haga clic en **Assign (Asignar)**.

# Integración con Dell Repository Manager (DRM)

OMIMSSC está integrado con DRM (de la versión 2.2 en adelante) y proporciona la información de inventario de los servidores existentes desde el dispositivo OMIMSSC a DRM. Mediante la información de inventario, puede crear un repositorio personalizado en DRM y establecerlo como origen de actualizaciones en el dispositivo OMIMSSC a fin de que realice trabajos de actualización del firmware en los servidores o grupos de servidores. Para obtener más información sobre la creación de un repositorio en DRM, consulte los documentos de *Dell Repository Manager*.

## Acerca de esta tarea

**NOTA:** Después de realizar la actualización de OMIMSSC, vuelva a integrar DRM con el dispositivo OMIMSSC para ver la información más reciente sobre los servidores.

Para crear un repositorio para el dispositivo OMIMSSC mediante DRM:

## Pasos

- 1 Abra la versión de **Dell Repository Manager Data Center**.
- 2 Haga clic en **My Repositories (Mis repositorios)**, haga clic en **New (Nuevo)** y, a continuación, haga clic en **Dell Console Integration (Integración de la consola Dell)**.
- 3 Introduzca la dirección **URL (API de Rest)** en el siguiente formato `https:// IP address of appliance/genericconsolerepository/` y haga clic en **Next (Siguiendo)**.
- 4 Proporcione los datos de **User Name (Nombre de usuario)** y **Password (Contraseña)** que se utilizaron en el dispositivo OMIMSSC, haga clic en **Ok (Aceptar)** y, luego, haga clic en **Ok (Aceptar)**.

# Mantenimiento

Mediante la página **Centro de mantenimiento**, puede exportar inventario de servidores y programar trabajos para actualizar los servidores, recuperar los servidores a un estado anterior exportando su configuración anterior, aplicar las mismas configuraciones que las del componente anterior en elementos sustituidos, y exportar registros de LC para la solución de problemas.

Temas:

- [Acerca de las actualizaciones del firmware](#)
- [Recuperación](#)
- [Cómo aplicar el firmware y los ajustes de configuración](#)
- [Recopilación de registros de LC](#)
- [Exportación de inventario](#)

## Acerca de las actualizaciones del firmware

Es posible mantener actualizadas las versiones de firmware de los componentes del servidor Dell EMC como se recomienda. Cree orígenes de actualización y grupos de actualizaciones personalizados, o utilice los grupos de actualización predefinidos para actualizar el firmware. Puede crear y programar trabajos de actualizaciones de firmware, y programar notificaciones para recibir alertas cuando hay nuevos catálogos disponibles en el origen de actualización. Se proporciona un informe comparativo para la versión del firmware existente y la versión de referencia. De acuerdo con esta información, puede crear un archivo de inventario. Además, puede filtrar la información según el tipo de actualizaciones, los componentes del servidor y los modelos de servidores. Puede realizar actualizaciones solo en los servidores con hardware compatible, ya que las actualizaciones de la iDRAC están disponibles solo para la versión mínima compatible y las versiones posteriores.

**ⓘ NOTA:** Después de actualizar a la versión más reciente de OMIMSSC, si ocurre un error en la conexión a <ftp.dell.com> o <downloads.dell.com>, el origen de actualizaciones FTP o HTTP en línea predeterminado de Dell no podrá descargar el archivo del catálogo y, por lo tanto, el informe comparativo no estará disponible. Para ver un informe comparativo, edite el origen de actualizaciones FTP o HTTP en línea predeterminado de Dell, cree credenciales de proxy y, luego, seleccione estas opciones en el menú desplegable **Select Update Source (Seleccionar origen de actualizaciones)**. Para obtener más información sobre la edición de un origen de actualizaciones, consulte [Modificación de un origen de actualizaciones](#).

OMIMSSC proporciona las siguientes acciones de actualización en la página del **Maintenance Center (Centro de mantenimiento)**:

- **Downgrade (Degradación).** Existe una versión anterior disponible en el origen de actualizaciones y puede degradar el firmware a esta versión.
- **No Action Required (No se requiere ninguna acción).** La versión del firmware está en el mismo nivel que la del repositorio.
- **No Update Available (No hay actualizaciones disponibles).** No hay actualizaciones de firmware disponibles para el componente.
- **Upgrade - Optional (Actualización opcional).** Las actualizaciones constan de funciones nuevas o de actualizaciones de configuración específicas que son opcionales.
- **Upgrade - Urgent (Actualización urgente).** Las actualizaciones críticas utilizadas para resolver situaciones críticas de seguridad, rendimiento o reparación de errores en componentes como BIOS, etc., están disponibles.
- **Upgrade - Recommended (Actualización recomendada):** Las actualizaciones que implementen correcciones de errores o cualquier mejora en las funciones de OMIMSSC. También se incluyen las revisiones de compatibilidad con otras actualizaciones de firmware.

OMIMSSC proporciona los siguientes métodos para realizar las actualizaciones de firmware:

- **Update using DRM repository (Actualizar mediante el repositorio de DRM).** Exporte la información de inventario de los servidores detectados desde un dispositivo para preparar un repositorio en DRM. Para obtener más información acerca de cómo exportar la información de inventario, consulte [Exportación del inventario](#).

- Después de crear un repositorio en DRM, seleccione los servidores correspondientes e inicie una actualización en los servidores. Tenga en cuenta otros factores, como las pruebas en entornos de prueba, las actualizaciones de seguridad, las recomendaciones de aplicación, los avisos de Dell, etc., para preparar las actualizaciones necesarias. Para obtener más información sobre la creación de un repositorio, consulte los documentos de *Dell Repository Manager* disponibles en [dell.com/support/home](https://dell.com/support/home).
- **Update using FTP or HTTP (Actualización mediante FTP o HTTP)**. Actualice cualquier componente específico a la actualización más reciente que se proporciona en el sitio FTP o HTTP. El Departamento de TI de Dell prepara un repositorio trimestralmente.
  - Integración con el catálogo en línea de Dell: Conéctese al FTP de Dell y descargue el archivo de catálogo del directorio de caché (si es un origen de actualización de FTP) o conéctese a `downloads.dell.com` (si es un origen de actualización de HTTP) y, luego, conviértalo en un inventario de referencia.
  - Vea el informe de comparación con el origen de actualizaciones, seleccione los servidores o componentes del servidor relevantes y, a continuación, inicie la actualización en los servidores.
- **Referencing firmware inventory and comparison (Inventario de firmware de referencia y comparación)**. Cree un archivo de inventario de referencia que contenga el inventario de firmware de los servidores o grupos de servidores seleccionados. Luego, puede comparar la información de inventario de los servidores que esté presente en el dispositivo con el archivo de inventario de referencia guardado. El archivo de inventario del servidor de referencia contiene información sobre el inventario de un único servidor del mismo tipo o modelo, o puede tener varios servidores de diferentes tipos o modelos.

## Aplicación de actualizaciones en los servidores

### Prerrequisitos

Antes de aplicar actualizaciones en servidores, asegúrese de que se cumplan las siguientes condiciones:

- Para actualizar servidores, está disponible un origen de actualizaciones en el sitio FTP o HTTP de Dell en línea o local, o en Dell Repository Manager (DRM).
- La cola de trabajos de la iDRAC se borra antes de aplicar las actualizaciones en los servidores donde se aplican las actualizaciones.
- El usuario de IG tiene privilegios de administrador local en todos los nodos del clúster.
- Para crear el repositorio de firmware, asegúrese de que se pueda acceder al servidor FTP donde está alojado OMIMSSC, de que no haya problemas de red y de proporcionar las credenciales correctas durante un trabajo de actualización de firmware.

### Acerca de esta tarea

- ① **NOTA:** Puede aplicar las actualizaciones de firmware a un único componente de un servidor, o a todo el entorno.
- ① **NOTA:** Si no hay actualizaciones ni degradaciones aplicables para un servidor o grupo de servidores, la actualización de firmware en los servidores no tendrá ningún efecto.
- ① **NOTA:** Cuando actualiza información a nivel de componentes, si la versión del firmware existente es igual a la versión del firmware del origen de actualización, no se producirá ninguna acción en dicho componente.
- ① **NOTA:** Puede aplicar actualizaciones inmediatas o programar las actualizaciones en servidores o en un grupo de servidores mediante la creación de trabajos de actualización del firmware. Los trabajos creados para las actualizaciones aparecen en la lista de la página Jobs and Logs Center (Centro de trabajos y registros).
- ① **NOTA:** No puede actualizar el firmware de CMC directamente desde el dispositivo OMIMSSC. Sin embargo, puede actualizar el firmware del servidor modular presente en CMC. Para actualizar el firmware de CMC, consulte la sección *Updating CMC firmware (Actualización del firmware de CMC)* de la *Guía del usuario de Dell PowerEdge M1000e Chassis Management Controller Firmware (Firmware de Dell PowerEdge M1000e Chassis Management Controller)*. Para actualizar el firmware de CMC en VRTX, consulte la sección *Updating firmware (Actualización de firmware)* en la *Guía del usuario de Dell Chassis Management Controller for Dell PowerEdge VRTX (Dell Chassis Management Controller para Dell PowerEdge VRTX)*. Para actualizar el firmware de CMC en FX2, consulte la sección *Updating firmware (Actualización de firmware)* en la *Guía del usuario de Dell Chassis Management Controller for Dell PowerEdge FX2 (Dell Chassis Management Controller para Dell PowerEdge FX2)*.
- ① **NOTA:** Puede degradar la versión de firmware a una versión sugerida seleccionando Allow Downgrade (Permitir degradación). Si no selecciona esta opción, no ocurrirá nada en el componente que requiere una degradación del firmware.

### Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**, seleccione el servidor o el grupo de servidores y un origen de actualizaciones y, luego, haga clic en **Run Update (Ejecutar actualización)**.
- 2 En **Update Details (Detalles de la actualización)**, proporcione el nombre y la descripción del trabajo de actualización de firmware.

- 3 En **Schedule Update (Programar actualización)**, seleccione una de las opciones siguientes:
  - **Run Now (Ejecutar ahora)**. Esta opción permite aplicar las actualizaciones ahora.
  - Seleccione la fecha y la hora para programar una actualización de firmware en el futuro.
- 4 Seleccione un método de actualización, que puede ser **Agent-free Update (Actualización sin agente)** o **Agent-free Staged Update (Actualización en etapas sin agente)** y, luego, haga clic en **Finish (Finalizar)**.
  - **Agent-free staged updates (Actualizaciones en etapas sin agente)**: Las actualizaciones del firmware que pueden aplicarse directamente, se implementan de inmediato y sin un reinicio del sistema. Las demás actualizaciones se aplican durante el reinicio del sistema. Las actualizaciones se realizan mediante la iDRAC. El dispositivo OMIMSSC supone que la actualización se ha realizado satisfactoriamente cuando la iDRAC así lo informa. El dispositivo OMIMSSC no interactúa con el servidor después de la aplicación de actualizaciones. Si ocurre un error en la operación de un solo servidor, fallará todo el trabajo de actualización.
  - **Agent-free updates (Actualizaciones sin agente)**: La actualización del firmware es una actualización fuera de banda con reinicio inmediato si es necesario.

**NOTA:** Las actualizaciones del grupo de actualización del clúster se realizan mediante el coordinador de actualización del clúster que está presente en el mismo sistema donde está instalado IG. El trabajo de actualización se envía a la función de Actualización compatible en clústeres (CAU) de Microsoft, independientemente de la selección realizada en el menú desplegable Update Method (Método de actualización). Para obtener más información, consulte [Actualizaciones mediante la CAU](#).

**NOTA:** Después de enviar un trabajo de actualización de firmware a la iDRAC, el dispositivo OMIMSSC interactúa con la iDRAC para conocer el estado del trabajo y proporciona actualizaciones de estado en la página Jobs and Logs (Trabajos y registros) del Portal para administradores. A veces, la iDRAC no proporciona ninguna actualización de estado en los trabajos a los que el dispositivo OMIMSSC les realiza un seguimiento. El dispositivo OMIMSSC espera un máximo de 6 horas y, si no hay respuesta de la iDRAC, considera que hubo un error en el trabajo de actualización de firmware.

## Actualizaciones mediante la CAU

Las actualizaciones en los servidores se realizan mediante coordinador de actualizaciones del clúster (que está presente en el mismo sistema donde está instalado IG), y no mediante la iDRAC. Las actualizaciones no son en etapas y se aplican de inmediato. Mediante la CAU, puede minimizar cualquier interrupción o inactividad del servidor, lo que permite una disponibilidad continua de la carga de trabajo. Por lo tanto, el servicio proporcionado por el grupo de clúster no se ve afectado de ningún modo. Para obtener más información sobre la CAU, consulte la sección Descripción general de la actualización compatible en clústeres en [technet.microsoft.com](http://technet.microsoft.com).

Antes de aplicar las actualizaciones en grupos de actualización del clúster, verifique el informe de disponibilidad del clúster en relación con lo siguiente:

- La conectividad con origen de actualización.
- La disponibilidad de los clústeres de conmutación por error.
- Asegúrese de que el sistema operativo Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016 esté instalado en todos los nodos del clúster de conmutación por error para admitir la función CAU.
- La configuración de las actualizaciones automáticas no está habilitada para instalar automáticamente actualizaciones en cualquier nodo del clúster de conmutación por error.
- La activación de una regla de servidor de seguridad que permita el apagado remoto en cada nodo del clúster de conmutación por error.
- El grupo de clústeres debe tener un mínimo de dos nodos.
- Compruebe la disponibilidad de actualización del clúster. Para obtener más información sobre la CAU, consulte la sección Requisitos y prácticas óptimas para la actualización compatible en clústeres en [technet.microsoft.com](http://technet.microsoft.com).
- Para una actualización a nivel de componentes, expanda los grupos de servidores a su nivel de componentes y haga clic en **Run Update (Ejecutar actualización)**.
- Cuando se realiza una actualización de firmware para la 11.ª generación de servidores PowerEdge, no es posible actualizar las versiones de firmware de la unidad de suministro de energía (PSU).

**NOTA:** Asegúrese de que no haya errores ni avisos importantes en el informe para aplicar el método de CAU.

Para obtener más información sobre la aplicación de las actualizaciones, consulte [Ejecutar actualización](#).

## Sondeo y notificación

Puede configurar las notificaciones de sondeo para recibir alertas cuando hay nuevos catálogos disponibles en el origen de actualizaciones predeterminado que el usuario ha seleccionado. El color de la campana de notificación cambia a anaranjado cuando hay un nuevo archivo de catálogo disponible en el origen de actualizaciones. Para reemplazar el catálogo guardado localmente en la caché disponible en el origen de actualizaciones, haga clic en el icono de campana. Después de que se sustituyen los antiguos catálogos por los más recientes, el color de la campana cambia a verde.

### Acerca de esta tarea

Para configurar la frecuencia de sondeo:

#### Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Polling and Notification (Sondeo y notificación)**.
- 2 Seleccione la frecuencia con la que se llevará a cabo el sondeo:
  - **Never (Nunca)**. Esta opción está seleccionada de manera predeterminada. Selecciónela para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualizaciones solamente una vez a la hora programada.
  - **Once a week (Una vez a la semana)**. Seleccione esta opción para recibir semanalmente actualizaciones sobre nuevos catálogos disponibles en el origen de actualizaciones.
  - **Once every 2 weeks (Una vez cada 2 semanas)**. Seleccione esta opción para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualizaciones una vez cada dos semanas.
  - **Once a Month (Una vez al mes)**. Seleccione esta opción para recibir mensualmente actualizaciones sobre nuevos catálogos disponibles en el origen de actualizaciones.

## Descripción general de origen de actualización

El origen de actualizaciones le permite seleccionar y aplicar las actualizaciones de orígenes de actualizaciones de Dell. Puede crear, ver y administrar los orígenes de actualizaciones. Los tipos de orígenes de actualizaciones admitidos son repositorio de DRM, FTP y HTTP. Puede crear un origen de actualizaciones DRM, HTTP o FTP y configurarlo como predeterminado.

Los orígenes de actualizaciones tienen los archivos de catálogo que contienen las actualizaciones de Dell (BIOS, firmware, aplicación, drivers y paquetes de drivers), y contienen el archivo ejecutable autocontenido denominado Dell Update Packages (DUP).

Puede comparar la información de inventario disponible en el origen de actualizaciones con la información de inventario de un servidor o grupo de servidores seleccionados y crear una versión de referencia. También puede cambiar la fuente de la actualización y comparar la información de inventario de los servidores o del grupo de servidores con la información de la versión disponible en el origen de actualizaciones seleccionado.

Se recomienda realizar una actualización a la versión más reciente de firmware para utilizar la seguridad, las correcciones de errores y las solicitudes de nuevas funciones. Dell publica trimestralmente las siguientes actualizaciones mediante catálogos de PDK publicados en el sitio FTP de Dell:

- BIOS y firmware del servidor
- Paquetes del controlador del sistema operativo certificados por Dell (para la implementación del sistema operativo)

## Origen de actualización predefinido y predeterminado

**DELL ONLINE CATALOG (CATÁLOGO EN LÍNEA DE DELL)** es un origen de actualizaciones predefinido de tipo FTP disponible en el dispositivo OMIMSSC después de una nueva instalación o actualización. No es posible eliminar ni cambiar el nombre de un origen de actualizaciones predefinido.

**DELL ONLINE HTTP CATALOG (CATÁLOGO HTTP EN LÍNEA DE DELL)** es un origen de actualizaciones predefinido disponible en el dispositivo OMIMSSC después de una nueva instalación o actualización. No es posible eliminar ni cambiar el nombre de este origen de actualizaciones predeterminado. Sin embargo, puede crear otro origen de actualizaciones y marcarlo como predeterminado.

**NOTA:** Después de instalar OMIMSSC, introduzca los detalles del proxy para el origen de actualizaciones de DELL ONLINE CATALOG (CATÁLOGO EN LÍNEA DE DELL) y DELL ONLINE HTTP CATALOG (CATÁLOGO HTTP EN LÍNEA DE DELL) y guárdelo.

## Probar conexión

Utilice **Test Connection (Probar la conexión)** para verificar si la ubicación del origen de actualización es accesible por medio de las credenciales mencionadas al crear el origen de actualización.

Puede crear un origen de actualización solo después de confirmar que se puede acceder a la ubicación del catálogo a través las credenciales proporcionadas.

## Configuración de FTP local

Para configurar el FTP local:

- 1 Cree una estructura de carpeta en el FTP local que sea una réplica exacta del FTP en línea **ftp.dell.com**.
- 2 Descargue el archivo **catalog.xml.gz** del FTP en línea y extraiga los archivos.
- 3 Abra el archivo **catalog.xml** y cambie **baseLocation** a la URL del FTP local y, a continuación, comprima el archivo con la extensión **.gz**. Por ejemplo, cambie **baseLocation (Ubicación básica)** de **ftp.dell.com** a **ftp.yourdomain.com**.
- 4 Coloque el archivo de catálogo y los archivos DUP en su carpeta de FTP local replicando la misma estructura que en **ftp.dell.com**.

## Configuración de HTTP local

- 1 Cree una estructura de carpetas en el FTP local que sea una réplica exacta de **downloads.dell.com**.
- 2 Descargue el archivo **catalog.xml.gz** del sitio HTTP en línea en la siguiente ubicación: **http://downloads.dell.com/catalog/catalog.xml.gz** y extraiga los archivos.
- 3 Extraiga el archivo **catalog.xml**, cambie **baseLocation** a la URL del HTTP local y, a continuación, comprima el archivo con la extensión **.gz**. Por ejemplo, cambie **baseLocation (Ubicación básica)** de **downloads.dell.com** al nombre de host o la dirección IP, por ejemplo, **hostname.com**.
- 4 Coloque el archivo de catálogo con el archivo de catálogo modificado y los archivos DUP en su carpeta HTTP replicando la misma estructura de **downloads.dell.com**.

## Visualización del origen de actualizaciones

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)**.
- 2 En **Maintenance Center (Centro de mantenimiento)**, haga clic en **Maintenance Settings (Configuración de mantenimiento)** y, a continuación, haga clic en **Update Source (Origen de actualización)**.

Aparecen todos los orígenes de actualizaciones creados junto con su descripción, tipo de origen, ubicación y nombre de perfil de credenciales.

## Creación de un origen de actualizaciones

### Prerrequisitos

- Según el tipo de origen de actualizaciones, asegúrese de que haya disponible un perfil de credenciales de Windows o FTP.
- Si creará un origen de actualizaciones de DRM, asegúrese de instalar y configurar DRM, y de que los roles de Administrador estén configurados.

### Pasos

- 1 En la consola de OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En la página **Update Source (Origen de actualizaciones)**, haga clic en **Create New (Crear nuevo)** y proporcione el nombre y la descripción del origen de actualizaciones.

- 3 Seleccione cualquiera de los siguientes tipos de orígenes de actualizaciones del menú desplegable **Source Type (Tipo de origen)**:
  - FTP Sources (Orígenes de FTP): Seleccione esta opción para crear un origen de actualizaciones de FTP local o en línea.
    - ① **NOTA: Si crea un origen de FTP, proporcione las credenciales de FTP junto con las credenciales de proxy si se puede acceder al sitio FTP con las credenciales de proxy.**
  - HTTP Sources (Orígenes de HTTP): Seleccione esta opción para crear un origen de actualizaciones de HTTP local o en línea.
    - ① **NOTA: Si está creando un origen de actualización de tipo HTTP, proporcione la ruta de acceso completa de catálogo con el nombre de catálogo y sus credenciales de proxy para acceder al origen de actualización.**
  - DRM Repository (Repositorio de DRM): Seleccione esta opción para crear un origen de actualización de repositorio local. Asegúrese de tener DRM instalado.
    - ① **NOTA: Si creará un origen de DRM, proporcione sus credenciales de Windows y asegúrese de que sea posible acceder a la ubicación compartida de Windows. En el campo de ubicación, proporcione la ruta de acceso completa del archivo de catálogo con el nombre de archivo.**
  - Inventory Output files (Archivos de salida de inventario): Seleccione esta opción para ver el inventario de firmware comparado con la configuración del servidor de referencia.
    - ① **NOTA: Solo puede ver un informe comparativo si usa los archivos de salida de inventario como origen de actualizaciones, ya que esto compara la información de inventario de un servidor con todos los demás servidores.**
- 4 En **Location (Ubicación)**, proporcione la URL del origen de actualizaciones de FTP o HTTP, y la ubicación compartida de Windows para DRM.
  - ① **NOTA: El sitio FTP local deberá replicar el sitio FTP en línea.**
  - ① **NOTA: El sitio HTTP local deberá replicar el sitio HTTP en línea.**
  - ① **NOTA: No es obligatorio incluir HTTP o HTTPS en la URL de un origen de FTP.**
- 5 Para acceder al origen de actualizaciones, seleccione el perfil de credenciales necesario en **Credential (Credenciales)**.
- 6 En **Proxy Credentials (Credenciales de proxy)**, seleccione las credenciales de proxy requeridas si se necesita un proxy para acceder al origen de FTP o HTTP.
- 7 (Opcional) Para que el origen de actualizaciones creado sea el predeterminado, seleccione **Make this as default source (Convertir en origen predeterminado)**.
- 8 Para verificar que sea posible acceder a la ubicación del origen de actualizaciones con las credenciales mencionadas, haga clic en **Test Connection (Probar conexión)** y, luego, en **Save (Guardar)**.
  - ① **NOTA: Puede crear el origen de actualizaciones solo después de la prueba de conexión sea satisfactoria.**

## Modificación del origen de actualizaciones

### Acerca de esta tarea

Mientras modifica un origen de actualizaciones, asegúrese de anotar y recordar los siguientes puntos:

- No se puede cambiar el tipo de un origen de actualizaciones ni su ubicación después de crearlo.
- Puede modificar un origen de actualizaciones incluso si el mismo está siendo utilizado por un trabajo en curso o programado o si se lo utiliza en una plantilla de implementación. Se mostrará un mensaje de advertencia al modificar el origen de actualizaciones en uso. Haga clic en **Confirm (Confirmar)** para continuar con los cambios.
- Cuando un archivo de catálogo se actualiza en el origen de actualizaciones, el archivo de catálogo en caché local no se actualiza automáticamente. Para actualizar el archivo de catálogo guardado en caché, edite o elimine el origen de actualizaciones y vuelva a crear el origen de actualizaciones.

### Paso

Seleccione el origen de actualizaciones que desea modificar, haga clic en **Edit (Editar)** y actualice el origen según sea necesario.

## Eliminación de origen de actualizaciones

### Acerca de esta tarea

No es posible eliminar un origen de actualizaciones cuando:

- El origen de actualizaciones es un origen de actualizaciones predefinido que pertenece a **Dell Online Catalog (Catálogo en línea de Dell)** y **DELL ONLINE HTTP CATALOG (CATÁLOGO HTTP EN LÍNEA DE DELL)**.
- Un trabajo en curso o programado utiliza el origen de actualizaciones.
- El origen de actualizaciones es un origen de actualizaciones predeterminado.

#### Paso

Seleccione el origen de actualizaciones que desea eliminar y haga clic en **Delete (Eliminar)**.

## Grupos de actualización

Los grupos de actualización son un grupo de servidores que requieren una administración similar de las actualizaciones. Existen dos tipos de grupos de actualización disponibles:

- Grupos de actualización predefinidos: Solo puede ver los servidores en el grupo. No puede crear, modificar ni eliminar los grupos de actualización predefinidos manualmente.
- Grupos de actualización personalizados: Puede crear y mantener los servidores en el grupo.

**NOTA:** Todos los grupos de servidores que existen en SCVMM aparecen en OMIMSSC, ya que no son específicos de cada usuario. Asegúrese de que tiene acceso para realizar cualquier operación en esos servidores.

### Grupos de actualización predefinidos

La descripción y el comportamiento de los grupos de actualización predefinidos son los siguientes:

**Generic update groups (Grupos de actualización genéricos):** Este grupo consta de hosts y servidores sin asignar que se actualizan en una sola sesión.

**All Update Groups (Todos los grupos de actualización):** Este grupo se compone de todos los grupos de servidores. Cualquier grupo presente en OMIMSSC es un miembro de todos los grupos de actualización. Este grupo es un grupo de actualización genérico.

**Default unassigned server update group (Grupo de actualización de servidor sin asignar predeterminado):** Este grupo consta de todos los servidores sin asignar que no forman parte de cualquier otro grupo. Este grupo es un grupo de actualización genérico. Los servidores se agregan al grupo de actualización de servidores sin asignar predeterminado después de:

- un descubrimiento nuevo o un redescubrimiento de servidores físicos (bare metal).
- una sincronización o resincronización, una vez que se elimina de SCVMM pero está presente en el dispositivo OMIMSSC.

**Cluster update group (Grupo de actualización del clúster):** Este grupo se compone de los clústeres de conmutación por error de Windows Server. Si un servidor modular pertenece a un clúster, se agregará al grupo de actualización del clúster. Si un servidor modular Dell PowerEdge de 12.<sup>a</sup> o 13.<sup>a</sup> generación es parte de clúster, la información de CMC también se agrega en el inventario en la página **Maintenance Center (Centro de mantenimiento)**.

Para conocer el grupo de actualización de clúster al que pertenece un servidor, consulte la página **Configuration and Deployment (Configuración e implementación)** donde se muestra el nombre de host y el FQDN de clúster de todos los servidores que aparecen en OMIMSSC.

**Host update group (Grupo de actualización de host):** Este grupo consta de servidores de host y las actualizaciones se aplican en una sola sesión, es decir, todos los servidores del grupo se actualizan a la vez.

**Default host update group (Grupo de actualización de host predeterminado):** Este grupo consta de todos los hosts detectados que no son parte de ningún otro grupo. Este grupo es un grupo de actualización de host.

**Chassis update group (Grupo de actualización del chasis):** Los servidores modulares que pertenecen a un chasis y no forman parte de ningún grupo de clúster se clasifican como grupos de actualización del chasis. Se detectan los servidores PowerEdge de 12.<sup>a</sup> o 13.<sup>a</sup> generación junto con su información de CMC. De manera predeterminada, un grupo se crea con el formato de nombre **Chassis-etiqueta-de-servicio-de-chasis-grupo**. For example, `Chassis-GJDC4BS-Group`. Si un servidor modular se elimina de un grupo de actualización del

clúster, se agregará el servidor al grupo de actualización del chasis junto con su información de CMC. Incluso si no existen servidores modulares en el grupo de actualización del chasis correspondiente (porque todos los servidores modulares en el chasis se encuentran en un grupo de actualización del chasis), el grupo de actualización del chasis seguirá existiendo, pero solo aparecerá información sobre CMC.

**Default Non-Windows Host Update group (Grupo de actualización de host predeterminado que no es de Windows):** Este grupo consta de servidores que no tienen el sistema operativo Windows.

## Grupos de actualización personalizado

Este grupo le permite crear, modificar y eliminar grupos de actualización. Sin embargo, solo puede agregar un servidor a un grupo de actualización personalizado desde **Default unassigned update groups (Grupos de actualización personalizados sin asignar)** y **Default host update groups (Grupos de actualización de host predeterminados)**. Después de agregar un servidor a un grupo de actualización personalizado, el servidor se eliminará del grupo de actualización predefinido y estará disponible únicamente en el grupo de actualización personalizado. Para agregar los servidores al grupo de actualización personalizado, busque los servidores requeridos mediante su etiqueta de servicio.

**NOTA:** Si se elimina un servidor de MSSC y ejecuta una sincronización de OMIMSSC con el MSSC inscrito, se elimina el servidor del grupo de actualización personalizado y se traslada al grupo predefinido correspondiente.

## Métodos de actualización

Puede aplicar actualizaciones en grupos de servidor seleccionados cuyo hardware sea compatible con OMIMSSC.

- Puede realizar las siguientes actualizaciones en los grupos de servidores:
  - **Actualizaciones en etapas sin agentes:** Actualizaciones del firmware organizadas en etapas. Las actualizaciones de firmware que pueden aplicarse de inmediato y que no requieren un reinicio se aplican inmediatamente. Las demás actualizaciones que requieren el reinicio del sistema se aplican en el momento de reiniciar el servidor. Las actualizaciones se llevan a cabo en lotes a la hora programada mediante la iDRAC. El tamaño del lote se determina cuando la actualización tiene lugar. Para comprobar si todas las actualizaciones se aplican, actualice el inventario. Si ocurre un error en la operación de un solo servidor, fallará todo el trabajo de actualización.
  - **Actualizaciones sin agente:** Se trata de la actualización fuera de banda con reinicio inmediato del servidor.
  - **Actualización compatible en clústeres (CAU):** Se automatiza el proceso de actualización usando la función CAU de Microsoft en grupos de actualización de clúster para mantener la disponibilidad del servidor. Para obtener más información sobre la CAU, consulte [Actualizaciones mediante CAU](#).

## Visualización grupos de actualización

Para ver grupos de actualización:

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En **Maintenance Settings (Configuración de mantenimiento)**, haga clic en **Update Groups (Actualizar grupos)**.  
Todos los grupos personalizados creados aparecen con el nombre, el tipo de grupo y la cantidad de servidores en el grupo.

## Creación de grupos actualización personalizados

- 1 En la consola de OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En **Maintenance Settings (Configuración de mantenimiento)**, haga clic en **Update Groups (Grupos de actualización)** y, a continuación, haga clic en **Create (Crear)**.  
Aparece la página **Firmware Update Group (Grupo de actualización del firmware)**.
- 3 Proporcione un nombre de grupo y la descripción, y seleccione el tipo de grupo de actualización que desee crear.  
Los grupos de actualización personalizados pueden tener servidores solamente de los siguientes tipos de grupos de actualización:
  - Grupo de actualización genérico. Se compone de servidores de los grupos de actualización sin asignar predeterminados y de grupos de actualización de host.

- Grupo de actualización de host. Se compone de servidores de grupos de actualización de host predeterminados.

También puede tener una combinación de servidores de los dos tipos de grupos de servidores.

- 4 Para agregar servidores al grupo de actualización, busque los servidores por medio de su etiqueta de servicio; para agregar servidores a la tabla **Servers Included in the Update Group (Servidores incluidos en el grupo de actualización)**, haga clic en la flecha hacia la derecha.
- 5 Para crear el grupo de actualización personalizado, haga clic en **Save (Guardar)**.

## Modificación de grupos actualización personalizados

### Acerca de esta tarea

Tenga en cuenta lo siguiente al modificar un grupo de actualización personalizado:

- No puede cambiar el tipo de un grupo de actualización después de haberlo creado.
- Para trasladar servidores de un grupo de actualización personalizado a otro, puede hacer lo siguiente:
  - a Eliminar el servidor de un grupo de actualización personalizado existente. Luego, se agregará automáticamente al grupo de actualización predefinido.
  - b Editar el grupo personalizado para agregarle el servidor y, después, buscar el servidor mediante la etiqueta de servicio.

### Pasos

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En **Maintenance Settings (Configuración de mantenimiento)**, haga clic en **Update Groups (Grupos de actualización)**, seleccione el grupo de actualización, y, a continuación, haga clic en **Edit (Editar)** para modificar el grupo de actualización.

## Eliminación de grupos actualización personalizados

### Acerca de esta tarea

Tenga en cuenta lo siguiente al eliminar un grupo de actualización personalizado en las siguientes circunstancias:

- No puede eliminar un grupo de actualización si dispone de un trabajo programado, en curso o a la espera.
- Puede eliminar un grupo de actualización incluso si los servidores están presentes en dicho grupo. Sin embargo, después de eliminar dicho grupo, los servidores se trasladan a sus respectivos grupos de actualización predefinidos.
- Elimine los trabajos programados asociados con un grupo de actualización personalizado antes de eliminar el grupo de servidores.

### Pasos

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En **Maintenance Settings (Configuración de mantenimiento)**, haga clic en **Update Groups (Grupos de actualización)**, seleccione el grupo de actualización, y, a continuación, haga clic en **Delete (Eliminar)** para eliminar el grupo de actualización.

## Aplicación de filtros

Aplique filtros para ver la información seleccionada en el informe de comparación.

### Acerca de esta tarea

El dispositivo OMIMSSC es compatible con tres categorías de filtros:

- **Nature Of Update (Tipo de actualización)**: Seleccione esta opción para filtrar y ver solamente el tipo seleccionado de actualizaciones en los servidores.
- **Component Type (Tipo de componente)**: Seleccione esta opción para filtrar y ver solamente los componentes seleccionados en los servidores.
- **Server Model (Modelo de servidor)**: Seleccione esta opción para filtrar y ver solamente los modelos de servidor seleccionados.

**ⓘ | NOTA:** No puede exportar e importar perfiles de servidor si se aplican los filtros.

**Para aplicar filtros:**

## Paso

En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**, haga clic en el menú desplegable de filtros y seleccione los filtros.

## Siguiente paso

### Para quitar los filtros:

En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)** y haga clic en **Clear Filters (Borrar filtros)** o anule la selección de las casillas de verificación.

# Visualización y actualización de inventario de firmware

Puede ver y actualizar el inventario de firmware de los servidores o de un grupo específico de servidores.

Puede ver el informe comparativo de un inventario de servidores o chasis en relación con un origen de actualizaciones seleccionado. Puede cambiar el origen de actualizaciones y ver el informe comparativo de la información de inventario de los servidores seleccionados, los grupos de servidores o los chasis en relación con el origen de actualizaciones modificado.

Puede actualizar el inventario de firmware para un servidor, un grupo de servidores o un chasis para ver la información más reciente. Al actualizar la información de componentes de un servidor, se actualiza toda la información de inventario del servidor.

**NOTA:** En el momento de la creación, se almacena en caché una copia local del archivo de catálogo en OMIMSSC. Por lo tanto, debe actualizar el archivo de catálogo para ver el informe comparativo más reciente. Para actualizar el archivo de catálogo, edite el origen de actualizaciones y guárdelo, o elimínelo y vuelva a crearlo.

**NOTA:** Los detalles del servidor, como Driver Pack Version (Versión de paquete de drivers) y Drivers Available For OS (Drivers disponibles para SO) no se actualizan en las propiedades de Dell Out of Band Controllers (Controladoras de Dell fuera de banda) (OOB) del servidor en la consola de SCCM al actualizar el inventario. Para actualizar la página OOB, sincronice OMIMSSC con SCCM.

**NOTA:** Al actualizar a esta versión de OMIMSSC, la información más reciente no aparece para servidores detectados en versiones anteriores. Para obtener la información más reciente del servidor y el informe comparativo correcto, vuelva a detectar los servidores.

Para ver o actualizar el inventario de firmware de un servidor o grupo de servidores:

- 1 En OMIMSSC, en **Maintenance Center (Centro de mantenimiento)**, seleccione un grupo de actualización en **Select Update Group (Seleccionar grupo de actualización)**.
- 2 (Opcional) Para cambiar el origen de actualizaciones, seleccione un origen de actualizaciones desde **Select Update Source (Seleccionar origen de actualizaciones)**.
- 3 Para ver la información de firmware de la versión actual, la versión de referencia y la acción de actualización recomendada por el dispositivo OMIMSSC, expanda el grupo de servidores desde **Device Group/Servers (Grupo de dispositivos/servidores)** a nivel de servidores y, luego, a nivel de componentes.

### **NOTA:**

Cuando visualiza la información de nivel de componentes, la información relacionada con la tarjeta de interfaz de red (NIC) de la 11.ª generación de servidores PowerEdge aparece del siguiente modo:

- Después de escoger el filtro **Urgent (Urgente)** en **Nature of Update (Naturaleza de la actualización)**, aparecerá un informe solo con los componentes que necesitan actualizaciones urgentes. Si este informe se exporta, también se exportan los componentes con una acción de degradación que, a su vez, tengan actualizaciones críticas.
- Cuando hay varias interfaces de red disponibles en una sola tarjeta NIC, solo existe una anotación para todas las interfaces en la lista **Component Information (Información del componente)**. Una vez aplicada la actualización del firmware, se actualizan todas las tarjetas NIC.
- Cuando se agrega una tarjeta NIC junto con las tarjetas existentes, la tarjeta NIC agregada recientemente se detalla como otra instancia en la lista **Component Information (Información del componente)**. Una vez aplicada la actualización del firmware, se actualizan todas las tarjetas NIC.

- 4 Seleccione el servidor o los grupos de servidores que desea actualizar y, a continuación, haga clic en **Refresh Inventory (Actualizar inventario)**.

# Recuperación

Puede guardar el perfil del servidor en el almacén de protección. Para ello, exporte el perfil e impórtelo al mismo servidor para restituirlo a un estado anterior.

## Almacén de protección

El almacén de protección es un lugar seguro donde puede exportar e importar perfiles del servidor para un servidor o un grupo de servidores. Puede guardar este perfil del servidor en una ubicación compartida de la red creando un almacén externo o en una tarjeta SD vFlash creando un almacén interno. Puede asociar un servidor o un grupo de servidores con solo un almacén de protección. Sin embargo, puede asociar un almacén de protección con muchos servidores o grupos de servidores.

## Creación del almacén de protección

### Prerequisito

Asegúrese de que se puede acceder a la ubicación del almacén.

### Pasos

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)** y, luego, haga clic en **Maintenance Settings (Configuración de mantenimiento)**.
- 2 En **Maintenance Center (Centro de mantenimiento)**, haga clic en **Protection Vault (Centro de protección)** y, a continuación, haga clic en **Create (Crear)**.
- 3 Seleccione el tipo de almacén de protección que desea utilizar y proporcione los detalles.
  - Si va a crear un almacén de protección de tipo **Network Share (Recurso compartido de red)**, proporcione una ubicación para guardar los perfiles, las credenciales para acceder a esta ubicación y una frase de contraseña para proteger el perfil.

**NOTA:** Este tipo de almacén de protección proporciona compatibilidad con el uso compartido de archivos de tipo sistema de archivos de Internet común (CIFS).

- Si va a crear un almacén de protección de tipo **vFlash**, proporcione la frase de contraseña para proteger el perfil.

## Modificación del almacén de protección

### Acerca de esta tarea

No puede modificar el nombre, la descripción, el tipo de almacén de protección y la frase de contraseña.

### Pasos

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)**. > **Maintenance Settings (Configuración de mantenimiento)** > **Protection Vault (Almacén de protección)**.
- 2 Para modificar el almacén, selecciónelo y haga clic en **Edit (Editar)**.

## Eliminación del almacén de protección

### Acerca de esta tarea

No puede eliminar un almacén de protección en las siguientes circunstancias:

- El almacén de protección está asociado con un servidor o un grupo de servidores.  
Para eliminar dicho almacén de protección, elimine el servidor o grupo de servidores y, luego, elimine el almacén de protección.
- Hay un trabajo programado relacionado con el almacén de protección. Sin embargo, para eliminar dicho almacén de protección, elimine el trabajo programado y, luego, elimine el almacén de protección.

## Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**. > **Maintenance Settings (Configuración de mantenimiento)** > **Protection Vault (Almacén de protección)**.
- 2 Seleccione el almacén que desea eliminar y haga clic en **Delete (Eliminar)**.

# Exportación de perfiles de servidor

Puede exportar un perfil de servidor, incluidas las imágenes del firmware instalado en los distintos componentes (como BIOS, RAID, NIC, iDRAC y Lifecycle Controller) y la configuración de dichos componentes. El dispositivo OMIMSSC crea un archivo con todas las configuraciones, que usted puede guardar en una tarjeta SD vFlash o en un recurso compartido de red. Seleccione el almacén de protección que desee para guardar este archivo. Puede exportar los perfiles de configuración de un servidor o un grupo de servidores inmediatamente o programar esta tarea para una fecha posterior. Además, puede seleccionar una opción de repetición adecuada para definir con qué frecuencia se exportarán los perfiles de servidores. En una instancia, puede programar solamente un trabajo de configuración de exportación para un grupo de servidores. No podrá realizar ninguna otra actividad en el servidor o grupo de servidores si sus perfiles de configuración se están exportando.

## Prerequisito

Deshabilite la opción **F1/F2 Prompt on Error (Petición de F1/F2 en caso de error)** en **BIOS Settings (Configuración del BIOS)**.

## Acerca de esta tarea

- ① **NOTA:** Asegúrese de que el trabajo Automatic Backup (Copia de seguridad automática) en la iDRAC no se haya programado al mismo tiempo.
- ① **NOTA:** No es posible exportar perfiles de servidor después de aplicar los filtros. Para exportar los perfiles de servidor, borre todos los filtros aplicados.
- ① **NOTA:** Para exportar los perfiles de servidor, debe tener la licencia Enterprise de la iDRAC.
- ① **NOTA:** Antes de exportar el perfil del servidor, asegúrese de que no se haya modificado la dirección IP del servidor. Si la dirección IP del servidor ha cambiado debido a cualquier otra operación, debe volver a detectar este servidor en OMIMSSC y, luego, programar el trabajo de exportación del perfil de servidor.

## Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**. Seleccione los servidores cuyos perfiles desee exportar y haga clic en **Export Server Profile (Exportar perfil del servidor)**.
- 2 En la ventana **Export Server Profile (Exportar perfil de servidor)**, proporcione los detalles del trabajo y seleccione un almacén de protección.

Para obtener más información sobre los almacenes de protección, consulte [Creación de un almacén de protección](#).

En **Schedule Export Server Profile (Programar exportación del perfil de servidor)**, seleccione una de las siguientes opciones:

- **Run Now (Ejecutar ahora)**. Seleccione esta opción para exportar inmediatamente la configuración de los servidores o grupos de servidores seleccionados.
- **Schedule (Programa)**: Defina una frecuencia para exportar la configuración del servidor del grupo de servidores seleccionado.
  - **Never (Nunca)**. Seleccione esta opción para exportar el perfil de servidor solo una vez durante la hora programada.
  - **Once a week (Una vez a la semana)**. Seleccione esta opción para exportar el perfil de servidor semanalmente.
  - **Once every 2 weeks (Una vez cada 2 semanas)**. Seleccione esta opción para exportar el perfil de servidor una vez cada dos semanas.
  - **Once every 4 weeks (Una vez cada 4 semanas)**. Seleccione esta opción para exportar el perfil de servidor una vez cada cuatro semanas.

# Importación de perfil del servidor

Puede importar un perfil del servidor que se ha exportado anteriormente para ese mismo servidor o grupo de servidores. La importación del perfil del servidor es útil para restaurar la configuración y el firmware de un servidor a un estado almacenado en el perfil. En tales casos,

puede sustituir el perfil del servidor en ese servidor o grupo de servidores importando un perfil del servidor previamente exportado de ese servidor o grupo de servidores.

### Acerca de esta tarea

Puede importar los perfiles de servidor de dos maneras:

- Quick import server profile (Perfil del servidor de importación rápida): Esta opción le permite importar automáticamente el último perfil de servidor exportado para ese servidor. Para esta operación, no es necesario que seleccione perfiles del servidor individuales para cada uno de los servidores.
- Custom import server profile (Perfil del servidor de importación personalizada): Esta opción le permite importar perfiles del servidor para cada uno de los servidores seleccionados individualmente. Por ejemplo, si la exportación del perfil de servidor se ha programado y el perfil de servidor se exporta todos los días, esta función le permite seleccionar un perfil de servidor específico que se importe de la lista de perfiles de servidor disponibles en el almacén de protección de ese servidor.

### Notas de importación de perfil de servidor:

- Puede importar un perfil del servidor desde una lista de perfiles del servidor exportados para ese servidor solamente. No es posible importar los mismos perfiles del servidor para diferentes servidores o grupos de servidores. Si intenta importar el perfil del servidor de otro servidor o grupo de servidores, ocurrirá un error en el trabajo de importación del perfil del servidor.
- Si una imagen de perfil de servidor no está disponible para un servidor o grupo de servidores en particular, y se intenta realizar un trabajo de importación de perfil de servidor de ese servidor o grupo de servidores en particular, ocurrirá un error en el trabajo de importación de perfil de servidor en aquellos servidores que tengan perfil del servidor. Un mensaje de registro se agregará en el registro de actividades con los detalles del error.
- Después de exportar un perfil de servidor, si algún componente se elimina del servidor y, luego, se inicia un trabajo de importación de perfil, toda la información de componentes se restaura, pero se omite la información sobre componentes faltante. Esta información no está disponible en el registro de actividades de OMIMSSC. Para conocer más sobre los componentes faltantes, consulte **LifeCycle Log (Registro de LifeCycle)** en iDRAC.
- No es posible importar un perfil del servidor después de aplicar los filtros. Para importar los perfiles de servidor, borre todos los filtros aplicados.
- Para importar los perfiles de servidor, debe tener la licencia Enterprise de la iDRAC.

### Pasos

- 1 En OMIMSSC, en **Maintenance Center (Centro de mantenimiento)**, seleccione los servidores cuyos perfiles desea importar y haga clic en **Import Server Profile (Importar perfil de servidor)**.
- 2 Proporcione los detalles y seleccione la opción **Import Server Profile Type (Tipo de importación del perfil del servidor)** que desee.

① **NOTA:** La opción predeterminada es **Preserve Data (Conservar los datos)**, que conserva la configuración del RAID existente en el servidor. Anule la selección de la casilla de verificación si desea aplicar la configuración del RAID almacenada en el perfil del servidor.

- 3 Para importar el perfil del servidor, haga clic en **Finish (Finalizar)**.

## Cómo aplicar el firmware y los ajustes de configuración

La función de sustitución de piezas actualiza automáticamente un componente de servidor sustituido a la versión de firmware necesaria o a la configuración de un componente anterior (o ambos). La actualización se produce de forma automática al reiniciar el sistema después de reemplazar el componente.

### Acerca de esta tarea

Para establecer los parámetros para sustitución de piezas:

### Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**, seleccione los servidores o el grupo de servidores y, luego, haga clic en **Configure Part Replacement (Configurar reemplazo de piezas)**. Aparecerá la ventana **Configuración de reemplazo de piezas**.
- 2 Puede escoger cualquier de las siguientes opciones para **CSIOR, Part Firmware Update (Actualización de firmware de pieza)** y **Part Configuration Update (Actualización de configuración de pieza)** y, luego, hacer clic en **Finish (Finalizar)**:

- Recopilación de inventario del sistema al reiniciar (CSIOR): recopila toda la información del componente en cada reinicio del sistema.
  - **Enabled (Activado):** la información sobre el inventario de software y hardware de los componentes del servidor se actualiza automáticamente durante cada reinicio del sistema.
  - **Disabled (Desactivado):** la información sobre el inventario de software y hardware de los componentes del servidor no se actualizan.
  - **Do not change the value on the server (No cambiar el valor en el servidor):** se conserva la configuración del servidor existente.
- Part firmware update (Actualización de firmware de pieza): Restaura, actualiza o degrada la versión de firmware del componente en función de la selección.
  - **Disabled (Desactivado):** La actualización del firmware de la pieza está deshabilitada y se aplica lo mismo al componente sustituido.
  - **Allow version upgrade only (Permitir solo la actualización de la versión):** Las versiones de firmware actualizadas se aplican al componente sustituido si la versión de firmware de la pieza nueva es anterior a la versión existente.
  - **Match firmware of replaced part (Hacer coincidir el firmware de la pieza reemplazada):** Se hace coincidir la versión de firmware del componente nuevo con la versión de firmware del componente original.
  - **Do not change the value on the server (No cambiar el valor en el servidor):** se conserva la configuración actual del componente.
- Part configuration update (Actualización de configuración de pieza): Restaura o actualiza la configuración del componente según lo que se seleccione.
  - **Disabled (Deshabilitado):** La actualización de la configuración de la pieza se deshabilita y la configuración guardada del componente anterior no se aplica al componente sustituido.
  - **Apply Always (Aplicar siempre):** La actualización de la configuración de la pieza se habilita y la configuración guardada del componente anterior se aplica al componente sustituido.
  - **Apply only if firmware matches (Aplicar solo si coincide el firmware):** La configuración guardada del componente anterior se aplica a los componentes sustituidos solo si sus versiones de firmware coinciden.
  - **Do not change the value on the server (No cambiar el valor en el servidor):** se conserva la configuración existente.

## Recopilación de registros de LC

### Acerca de esta tarea

Los registros de LC proporcionan antecedentes de actividades anteriores en un sistema administrado. Estos archivos de registro son útiles para los administradores del servidor, ya que proporcionan información detallada sobre las acciones que se recomiendan y demás información técnica que es útil para solucionar problemas. Existen varios tipos de información que ofrecen los registros de LC: alertas relacionadas con los cambios de configuración en los componentes de hardware del sistema, cambios del firmware debidos a una actualización de la versión o regreso a una versión anterior, piezas reemplazadas, advertencias sobre la temperatura, fecha y hora detalladas del momento en el que se inició la actividad, gravedad de la actividad, etc.

Existen dos opciones para recopilar registros de LC:

- Registros de LC activos. Se trata de los archivos de registro de LC recientes. Puede ver, buscar y exportar estos archivos de registro en el dispositivo. Puede programar un trabajo para recopilar los registros de LC en un dispositivo o un recurso compartido de red. Además, puede guardar una copia de seguridad del archivo de registro en el recurso compartido de red.
- Registros de LC completos. Estos registros contienen archivos de registro activos y archivados. Son grandes y, por lo tanto, se comprimen en formato `.gz` y se exportan a la ubicación especificada en un recurso compartido de red de CIFS.

### Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**. Seleccione un servidor o un grupo de servidores y haga clic en **Collect LC Logs (Recopilar registros de LC)**.
- 2 En **LC Log Collection (Recopilación de registros de LC)**, seleccione una de las siguientes opciones y haga clic en **Finish (Finalizar)**:
  - **Export Complete LC Logs (.gz) (Exportar registros de LC completos [.gz])**. Exporta los registros de LC activos y archivados a un recurso compartido de red de CIFS usando las credenciales de Windows.

Por ejemplo, `201607201030010597.xml.gz` es el nombre del archivo de LC, que incluye la fecha y la hora del archivo en la que se creó.

 **NOTA:** Asegúrese de que la carpeta compartida tenga espacio suficiente para guardar los registros de LC completos, ya que son archivos de gran tamaño.

**NOTA:** La exportación de registros de LC completos no se admite con servidores Dell PowerEdge de 11.ª generación.

**NOTA:** Los registros de LC se guardan en el siguiente formato: <YYYYMMDDHHMMSSSS>.<file format>

- **Export Active Logs (Run now) (Exportar registros activos [Ejecutar ahora]).** Seleccione esta opción para exportar los registros activos inmediatamente al dispositivo.
  - (Opcional) Habilite la opción **Back up LC logs on the network share (Realizar copias de seguridad de los registros de LC en el recurso compartido de red)** para guardar una copia de seguridad de los registros de LC en el recurso compartido de red de CIFS usando las credenciales de Windows.

**NOTA:** Asegúrese de actualizar iDRAC y LC a las versiones más recientes antes de exportar registros de LC activos para servidores Dell PowerEdge de 11.ª generación.

- **Schedule LC Log Collection (Recopilación de registros de LC programados).** Seleccione una fecha, hora y frecuencia para exportar los registros de LC activos.
  - (Opcional) Habilite la opción **Back up LC logs on the network share (Realizar copias de seguridad de los registros de LC en el recurso compartido de red)** para guardar una copia de seguridad de los registros de LC en el recurso compartido de red de CIFS usando las credenciales de Windows.

Las opciones disponibles para programar la frecuencia y determinar la frecuencia con la que desea recopilar los registros de LC son:

- **Never (Nunca).** Seleccione esta opción para exportar los registros de LC solo una vez a la hora programada.
- **Daily (Diariamente).** Seleccione esta opción para exportar los registros de LC diariamente a la hora programada.
- **Once a week (Una vez a la semana).** Seleccione esta opción para exportar los registros de LC una vez a la semana a la hora programada.
- **Once every 4 weeks (Una vez cada 4 semanas).** Seleccione esta opción para exportar los registros de LC una vez cada cuatro semanas a la hora programada.

**NOTA:** El archivo de registros de LC exportado se guarda con el nombre de carpeta de la etiqueta de servicio de ese servidor particular.

## Visualización de registros de LC

Puede ver todos los registros activos de LC, buscar descripciones detalladas y descargar los registros en formato CSV mediante la función Ver registros de LC.

### Prerequisito

Defina la configuración del navegador como se indica en [Configuración del navegador](#).

### Pasos

- 1 En OMIMSSC, haga clic en **Maintenance Center (Centro de mantenimiento)**. Seleccione un servidor o un grupo de servidores y haga clic en **View LC Logs (Ver registros de LC)**.
- 2 Todos los servidores en el grupo seleccionado y los servidores para los cuales se van a recopilar los registros de LC se enumeran con sus archivos de registro de LC. Haga clic en el nombre de un archivo para ver todas las entradas de registro del archivo de registro de LC específico de ese servidor. Para obtener más información, consulte [Descripción del archivo](#).
- 3 (Opcional) Utilice el cuadro de búsqueda para buscar la descripción en todos los archivos de registro y exportar el archivo en formato CSV.

Hay dos formas de buscar descripciones de mensajes en archivos LC:

- Haga clic en el nombre de un archivo para abrir el archivo de registro de LC y busque una descripción en el cuadro de búsqueda.
- Escriba un texto de descripción en el cuadro de búsqueda y, luego, visualice todos los archivos de LC que contengan el texto especificado.

**NOTA:** Si la descripción del mensaje del registro de LC es larga, el mensaje se truncará a 80 caracteres.

**NOTA:** El tiempo que aparece en los mensajes de registro de LC tiene la zona horaria de la iDRAC.

**NOTA:** Antes de descargar los registros de LC, agregue el dispositivo al sitio de intranet local.

Para agregar el dispositivo en **Local intranet (Intranet local)** en **Internet Explorer**:

- a Inicie el navegador, haga clic en **Tools (Herramientas)** y en **Internet Options (Opciones de Internet)**.
- b Haga clic en **Security (Seguridad) > Local intranet (Intranet local) > Sites (Sitios)**. Aparecerá la página **Local intranet (Intranet local)**.
- c Haga clic en **Advanced (Avanzado)**, escriba la URL del dispositivo y haga clic en **Add (Agregar)**.

## Descripción del archivo

Utilice esta ventana para ver información detallada sobre las acciones recomendadas y otro tipo de información técnica que es útil para fines de alerta o de seguimiento de un servidor en particular.

Para ver el contenido de un archivo, haga clic en un nombre de archivo:

- Puede buscar descripciones específicas de los mensajes.
- Puede ver los archivos de registro en la ventana o descargar el archivo para ver más mensajes de registro.
- Puede ver los comentarios de un usuario para una actividad.

**NOTA:** Cuando se utiliza la opción de búsqueda, solo se exportan los resultados de la búsqueda a un archivo .CSV.

**NOTA:** Si el mensaje es largo, se truncará a 80 caracteres.

**NOTA:** Haga clic en Message ID (Id. de mensaje) para ver más información sobre el mensaje.

## Exportación de inventario

En OMIMSSC, puede exportar el inventario de servidores seleccionados o un grupo de servidores a un archivo de formato XML o CSV. Puede guardar esta información en un directorio compartido de Windows o en un sistema de administración.

### Prerequisito

**NOTA:** Puede importar el archivo XML en DRM y crear un repositorio con base en el archivo de inventario y crear una configuración de referencia.

Defina la configuración del navegador como se indica en [Configuración del navegador](#).

### Acerca de esta tarea

**NOTA:** Cuando se selecciona solo la información del componente de un servidor y la exporta, la información de inventario completa del servidor se exporta.

### Pasos

- 1 En **OMIMSSC**, haga clic en **Maintenance Center (Centro de mantenimiento)**.
- 2 Seleccione los servidores cuyo inventario desea exportar y seleccione el formato en el menú desplegable **Export Inventory (Exportación de inventario)**.

El archivo exportado se compone de información detallada sobre, por ejemplo, los grupos de servidores, la etiqueta de servicio del servidor, el nombre de host o la dirección IP, el modelo de dispositivo, el nombre de componente, versión de firmware actual en ese componente, la versión de firmware del origen de actualizaciones y las actualizaciones realizadas en ese componente.

### Pasos siguientes

Para crear un repositorio de DRM después de exportar el archivo XML, siga estos pasos:

- 1 Haga clic en **My Repositories (Mis repositorios)**, > **New (Nuevo) > Dell Modular Chassis inventory (Inventario de chasis modular de Dell)**.
- 2 Introduzca un nombre y una descripción en la sección **Base Repository (Repositorio básico)** y haga clic en **Next (Siguiendo)**.
- 3 Para seleccionar el archivo de inventario exportado de un dispositivo, haga clic en **Browse (Examinar)** en la sección **Modular Chassis Inventory (Inventario de chasis modular)** y, luego, haga clic en **Next (Siguiendo)**.

Para obtener más información sobre la creación de un repositorio, consulte los documentos de *Dell Repository Manager* disponibles en [dell.com/support/home](http://dell.com/support/home).

# Visualización de información en OMIMSSC

Puede ver toda la información sobre las actividades iniciadas en OMIMSSC junto con el estado de progreso de un trabajo y sus subtareas mediante la página **Centro de tareas y registros**. Además, puede filtrar y ver los trabajos de una categoría particular. Puede ver los trabajos desde el Portal para administradores de OMIMSSC y la extensión de la consola de OMIMSSC.

- Portal para administradores: Aparecen los trabajos iniciados de todos los usuarios de OMIMSSC
- Consola de OMIMSSC: Aparecen los trabajos específicos de un usuario y una consola

Los usuarios o el sistema definen los nombres de los trabajos, y los nombres de las subtareas se definen según la dirección IP o el nombre de host del servidor administrado. Amplíe la subtask para ver los registros de actividad de ese trabajo. Hay cuatro categorías de trabajos:

- Running (En ejecución): Aparecen todos los trabajos que actualmente están en ejecución o en estado de progreso.
- History (Historial): muestra todas las tareas que se ejecutaron anteriormente con su estado de tarea.
- Scheduled (Programados): Aparecen todos los trabajos programados para una fecha y hora futuras. Además, permite cancelar los trabajos programados.
- Generic Logs (Registros genéricos): Aparecen los mensajes de registro comunes y específicos del dispositivo OMIMSSC que no pertenecen a una subtask en particular y otras actividades para cada usuario que especifique el nombre de usuario y el FQDN de la consola.
  - Appliance Log Messages (Mensajes de registro del dispositivo): Aparecen todos los mensajes de registro específicos del dispositivo OMIMSSC, como reiniciar el dispositivo OMIMSSC. Puede ver esta categoría de mensajes solo desde el Portal para administradores.
  - Generic Log Messages (Mensajes de registro genérico): muestra todos los mensajes de registro que son comunes para las tareas que se muestran en las pestañas **Running (En ejecución)**, **History (Historial)** y **Scheduled (Programado)**. Estos registros son específicos para una consola y un usuario.  
Por ejemplo, si un trabajo de actualización de firmware de un grupo de servidores se encuentra en progreso, en la ficha aparecen los mensajes de registro que pertenecen a la creación del repositorio de Server Update Utility (SUU) de ese trabajo.

Los distintos estados de trabajos definidos en el dispositivo OMIMSSC son los siguientes:

- Canceled (Cancelado): El usuario canceló manualmente el trabajo o se canceló cuando se reinició el dispositivo OMIMSSC.
- Successful (Correcto): El trabajo se completó satisfactoriamente.
- Failed (Error): No se pudo completar el trabajo.
- In Progress (En curso): la tarea se está ejecutando.
- Scheduled (Programada): la tarea se ha programado para otra fecha.

**NOTA:** Si varios trabajos se envían al mismo tiempo al mismo servidor, ocurre un error. Por lo tanto, asegúrese de programar los trabajos en diferentes momentos.

- Waiting (En espera): la tarea está en cola para comenzar a ejecutarse.
- Recurring Schedule (Programa periódico): tarea recurrente después de un intervalo fijo de tiempo.

Temas:

- [Visualizar trabajos](#)
- [Administración de trabajos](#)

# Visualizar trabajos

## Acerca de esta tarea

Puede ver todos los trabajos creados en OMIMSSC junto con información sobre su estado.

## Pasos

- 1 En OMIMSSC, haga clic en **Jobs and Logs Center (Centro de trabajos y registros)**.
- 2 Para ver una categoría específica de trabajos, como **Scheduled (Programado)**, **History (Historial)** o **Generic (Genérico)**, haga clic en la ficha deseada.

Expanda el trabajo para ver todos los servidores incluidos en el trabajo. Amplíe todavía más para ver los mensajes de registro para ese trabajo.

**NOTA:** Todas las tareas relacionadas con los mensajes de registro se muestran en la lista en la pestaña **Generic (Genérica)** y no en las pestañas **Running (En ejecución)** o **History (Historial)**.

- 3 (Opcional) Aplique filtros para ver diferentes categorías de trabajos y podrá ver su estado en la columna **Status (Estado)**.

# Administración de trabajos

## Prerequisito

Asegúrese de que el trabajo esté en el estado **Scheduled (Programado)**.

## Pasos

- 1 En OMIMSSC, realice cualquiera de las siguientes tareas:
  - En el panel de navegación, haga clic en **Maintenance Center (Centro de mantenimiento)** y, a continuación, haga clic en **Administrar tareas**.
  - En el panel de navegación, haga clic en **Jobs and Log Center (Centro de tareas y registros)** y, a continuación, haga clic en la pestaña **Scheduled (Programado)**.
- 2 Seleccione los trabajos que desee cancelar, haga clic en **Cancel (Cancelar)** y, luego, haga clic en **Yes (Sí)** para confirmar.

## Solución de problemas

### Temas:

- La opción de implementación no aparece en la secuencia de tareas
- Creación de grupos de chasis VRTX duplicados
- El grupo de actualización de clúster vacío no se elimina durante el descubrimiento automático o la sincronización
- Error de creación de origen de actualización
- Error de actualización de firmware porque la cola de trabajos está llena
- Error de actualización del firmware en grupo actualización de clúster
- Error al actualizar el firmware en 11.a generación de servidores
- Error al actualizar el firmware utilizando la fuente de actualización de DRM
- Error de un trabajo programado en un grupo de actualización
- Error al aplicar la Plantilla operativa
- Error de acceso al recurso compartido de CIFS mediante el nombre de host
- Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema
- Error al crear un repositorio durante una actualización del firmware
- Error al eliminar un grupo de actualización personalizado
- Error de visualización de trabajos y registros
- Error al exportar registros de LC en formato CSV
- Error al exportar perfiles de servidores
- Error al mostrar el logotipo de Dell EMC en el Portal para administradores de OMIMSSC
- Error al ver los registros de LC
- Actualización del firmware en algunos componentes independientemente de la selección
- Error de implementación de hipervisores
- Error de implementación del hipervisor debido a archivos de controlador retenidos en el recurso compartido de biblioteca
- Error en la implementación del hipervisor en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory
- Credenciales incorrectas durante la detección
- Problema de instalación de IG mientras se ejecutan varias instancias del instalador en el mismo servidor
- La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas
- La información de inventario más reciente no aparece incluso después una actualización del firmware
- Error 21119 de SCVMM VMM al agregar servidores Active Directory

## La opción de implementación no aparece en la secuencia de tareas

La opción **Deploy (Implementar)** no aparece en una secuencia de tareas existente después de desinstalar y reinstalar la extensión de la consola de OMIMSSC para SCCM.

Como una solución, abra la secuencia de tareas para editarla, vuelva a habilitar la opción **Apply (Aplicar)** y haga clic en **OK (Aceptar)**. La opción **Deploy (Implementar)** volverá a aparecer.

Para volver a activar la opción **Aplicar**:

- 1 Haga clic con el botón derecho en la secuencia de tareas y seleccione **Editar**.
- 2 Seleccione **Reiniciar en Windows PE**. En la sección **Descripción**, escriba cualquier carácter y bórralo para que el cambio no se guarda.
- 3 Haga clic en **OK** (Aceptar).  
Esto reactiva la opción **Aplicar**.

## Creación de grupos de chasis VRTX duplicados

Cuando los servidores modulares que antes estaban en otro chasis se agregan a un chasis VRTX y se detectan, los servidores modulares llevan la información de la etiqueta de servicio del chasis anterior y crean un grupo de chasis VRTX duplicado en el dispositivo.

Para solucionar este problema, realice lo siguiente:

- 1 Extraiga un servidor modular de un chasis y agréguelo a otro chasis. Para obtener más información, consulte la sección Módulos de servidor en el *Manual del propietario de Dell PowerEdge VRTX Enclosure (Gabinete Dell PowerEdge VRTX)*.
- 2 Configure CMC. Para obtener más información, consulte Instalación y configuración de CMC en la *Guía del usuario de Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX (Chassis Management Controller versión 2.1 para Dell PowerEdge VRTX)* disponible en [dell.com/support/home](http://dell.com/support/home).

Después de hacer las tareas anteriores, si hay entradas duplicadas del grupo de chasis, realice lo siguiente a modo de solución:

- 1 Active la función CSIOR y restablezca el iDRAC en el servidor modular recién agregado.
- 2 Elimine manualmente todos los servidores del grupo de chasis VRTX y, a continuación, vuelva a descubrir los servidores.

## El grupo de actualización de clúster vacío no se elimina durante el descubrimiento automático o la sincronización

Cuando se detecta un grupo del clúster en el dispositivo, se crea un grupo actualización del clúster en el **Maintenance Center (Centro de mantenimiento)** con todos los servidores que aparecen en el grupo de actualización del clúster. Más adelante, si se eliminan todos los servidores de este clúster mediante SCVMM y se realiza una operación de detección automática o una sincronización con SCVMM, no se eliminará el grupo de actualización del clúster vacío en **Maintenance Center (Centro de mantenimiento)**.

Para solucionar este problema y vaciar el grupo de servidores vacío, vuelva a descubrir los servidores.

## Error de creación de origen de actualización

Cuando se modifica la configuración de red del sistema de nombres de dominio (DNS) del dispositivo, ocurre un error en la creación del origen de actualizaciones de tipo HTTP o FTP.

Para solucionar este problema, reinicie el dispositivo y, luego, cree el origen de actualizaciones de tipo HTTP o FTP.

## Error de actualización de firmware porque la de cola de trabajos está llena

Ocurre un error en los trabajos de actualización del firmware enviados desde el dispositivo a la iDRAC, y el registro principal del dispositivo muestra el siguiente error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s)`.

Para solucionar este problema, elimine manualmente los trabajos terminados en la iDRAC y vuelva a intentar realizar el trabajo de actualización de firmware. Para obtener más información sobre cómo eliminar trabajos en la iDRAC, consulte la documentación de la iDRAC en [dell.com/support/home](http://dell.com/support/home).

## Error de actualización del firmware en grupo actualización de clúster

Después de programar un trabajo de actualización de firmware en un grupo de actualización de clúster, puede ocurrir un error en dicho trabajo por diversos motivos (por ejemplo, que no fuera posible acceder a IG, que el grupo de clúster deja de responder o que el trabajo de actualización de firmware se haya cancelado en la CAU debido a un trabajo en curso). Si esto sucede, los DUP se descargan y colocan en cada nodo del clúster de servidores que pertenezca al grupo de clústeres. Todos los archivos DUP se guardarán en la carpeta denominada Dell que consume memoria.

Para solucionar este problema, elimine todos los archivos de la carpeta Dell y, a continuación, programe un trabajo de actualización de firmware.

## Error al actualizar el firmware en 11.ª generación de servidores

Es posible que un trabajo de actualización de firmware que se haya iniciado en la 11.ª generación de servidores PowerEdge falle debido a versiones incompatibles de la iDRAC y LC con el siguiente error: `WSMan command failed to execute on server with iDRAC IP <IP address>`

Para solucionar este problema, actualice el iDRAC y LC a las versiones más recientes y, a continuación, inicie la tarea de actualización de firmware.

## Error al actualizar el firmware utilizando la fuente de actualización de DRM

Es posible que ocurra un error en el trabajo de actualización de firmware si utiliza el origen de actualizaciones de DRM con acceso insuficiente a las carpetas del recurso compartido. Si el perfil de credenciales de Windows suministrado al crear el origen de actualizaciones de DRM no forma parte del grupo de administradores de dominio o del grupo de administradores locales, aparecerá el siguiente mensaje de error: `Local cache creation failure.`

Para solucionar este problema, realice lo siguiente:

- 1 Después de crear el repositorio de DRM, haga clic con el botón derecho del mouse en la carpeta, luego haga clic en la pestaña **Security (Seguridad)** y, a continuación, haga clic en la pestaña **Advanced (Avanzada)**.
- 2 Haga clic en **Enable inheritance (Habilitar herencia)** y seleccione la opción **Replace all child object permission entries with inheritable permission entries from this object (Sustituir todas las entradas con permisos de objetos secundarios con entradas de permisos heredables de este objeto)** y, a continuación, comparta la carpeta con **Everyone (Todos)** con permiso de lectura y escritura.

## Error de un trabajo programado en un grupo de actualización

Después de programar un trabajo en un grupo de actualización, si todos los servidores se mueven fuera del grupo de actualización y no hay servidores que estén presentes en el grupo de actualización, fallará el trabajo programado.

Para solucionar este problema, cancele el trabajo programado, agregue los servidores a otro grupo de actualización y, a continuación, programe un trabajo en el grupo de actualización.

## Error al aplicar la Plantilla operativa

Después de enviar el trabajo **Deploy** the Operational Template (Implementar la plantilla operativa) en los servidores seleccionados, si los atributos o valores de atributo no son apropiados para el archivo .CSV seleccionado o la dirección IP o las credenciales de la iDRAC se

modifican debido a la plantilla, el trabajo en la iDRAC se realizará de manera satisfactoria. Sin embargo, el estado de este trabajo en OMIMSSC aparecerá como no satisfactorio debido a que el archivo .CSV no es válido, o que no es posible realizar un seguimiento del trabajo debido a los cambios en el servidor de destino de la iDRAC.

Para solucionar este problema, asegúrese de que el archivo .CSV seleccionado tenga todos los atributos y valores de atributo adecuados, y la dirección IP o las credenciales de la iDRAC no se modifiquen debido a la plantilla.

## Error de acceso al recurso compartido de CIFS mediante el nombre de host

Es posible que los servidores modulares no puedan acceder al recurso compartido de CIFS mediante el nombre de host para realizar cualquier trabajo de OMIMSSC.

Para solucionar este problema, especifique la dirección IP del servidor que tiene el recurso compartido de CIFS.

## Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema

Después de instalar y configurar o de actualizar el dispositivo, es posible que falle el intento de acceder al sitio FTP con un **catálogo en línea de Dell** de origen de actualizaciones creado por el sistema si se necesitan credenciales de proxy.

Para acceder al sitio FTP con el **Catálogo en línea de Dell** como origen de actualizaciones, edite y agregue las credenciales de proxy.

## Error al crear un repositorio durante una actualización del firmware

La creación de un repositorio puede fallar durante una actualización de firmware debido a problemas de red, credenciales inadecuadas o falta de acceso al servidor, etc.

Para solucionar este problema, asegúrese de que se pueda acceder al servidor FTP desde donde está alojado el dispositivo, de que no haya problemas de red y de proporcionar las credenciales correctas durante una actualización de firmware.

## Error al eliminar un grupo de actualización personalizado

Después de programar un trabajo en un servidor que pertenezca a un grupo de actualización personalizado, si el servidor se elimina de SCVMM y se realiza una sincronización, el servidor se elimina del grupo de actualización personalizado y se mueve al grupo predefinido correspondiente. No es posible eliminar dichos grupos de actualización personalizados, ya que están asociados con un trabajo programado.

Para solucionar este problema, para eliminar este grupo de actualización personalizado, elimine el trabajo programado de la página de trabajos y, a continuación, elimine el grupo de actualización personalizado.

## Error de visualización de trabajos y registros

El **Jobs and Logs Center (Centro de trabajos y registros)** no aparece en las extensiones de la consola de OMIMSSC.

Para solucionar este problema, vuelva a inscribir la consola.

# Error al exportar registros de LC en formato CSV

Al ver registros de LC, si intenta descargar archivos de registro al formato CSV, la operación de descarga falla.

Para solucionar este problema, agregue el FQDN del dispositivo en el navegador, en el sitio de intranet local. Para obtener más información sobre cómo agregar el dispositivo en la intranet local, consulte la sección [Visualización de registros de LC](#).

## Error al exportar perfiles de servidores

Después de programar un trabajo de exportación de perfil de servidor, el perfil de servidor no se ha exportado, y aparece el siguiente mensaje de error: "The selectors for the resource are not valid (Los selectores para el recurso no son válidos)".

Para solucionar este problema, restablezca la iDRAC y, luego, programe el trabajo de exportación de perfiles de servidor. Para obtener más información, consulte los documentos sobre la iDRAC disponibles en [dell.com/support/manuals](http://dell.com/support/manuals):

## Error al mostrar el logotipo de Dell EMC en el Portal para administradores de OMIMSSC

Cuando el Portal para administradores de OMIMSSC se inicia en un navegador Internet Explorer predeterminado de Windows 2016, dicho portal no aparece con el logotipo de Dell EMC.

Para solucionar este problema, realice una de las acciones siguientes:

- Actualice el navegador Internet Explorer a la versión más reciente.
- Elimine el historial de navegación y, luego, agregue la URL del Portal para administradores a la lista de favoritos del navegador.

## Error al ver los registros de LC

Después de recopilar los registros de LC, cuando vea el archivo de registro de LC de un servidor, aparecerá el siguiente mensaje de error: "Failed to perform the requested action. For more information see the activity log".

Para solucionar este problema, restablezca la iDRAC y, luego, recopile y vea los registros de LC. Para obtener más información, consulte los documentos sobre la iDRAC disponibles en [dell.com/support/manuals](http://dell.com/support/manuals):

## Actualización del firmware en algunos componentes independientemente de la selección

Los mismos componentes en servidores idénticos se actualiza durante una actualización del firmware independientemente de la selección de los componentes realizada en servidores individuales. Este comportamiento se observa en los servidores PowerEdge de 12.<sup>a</sup> y 13.<sup>a</sup> generación con licencia Enterprise de iDRAC.

Para solucionar este problema, realice una de las acciones siguientes:

- Para evitar actualizaciones irrelevantes en servidores idénticos, aplique componentes comunes en servidores idénticos y, a continuación, aplique los componentes específicos por separado en los servidores individuales.
- Realice las actualizaciones en etapas con tiempos de interrupción planificados para realizar la actualización de firmware necesaria.

## Error de implementación de hipervisores

La implementación del hipervisor falla y el registro de actividades muestra el siguiente error: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

Este error puede ocurrir debido a alguna de estas razones:

- El estado de Dell Lifecycle Controller es defectuoso.

Como solución, inicie sesión en la interfaz de usuario de iDRAC y restablezca Lifecycle Controller.

Después de restablecer Lifecycle Controller, si todavía experimenta el mismo problema, pruebe con la siguiente alternativa.

- El antivirus o el servidor de seguridad pueden restringir la ejecución correcta del comando **WINRM**.

Consulte el siguiente artículo de KB para solucionar este problema: [support.microsoft.com/kb/961804](https://support.microsoft.com/kb/961804).

## Error de implementación del hipervisor debido a archivos de controlador retenidos en el recurso compartido de biblioteca

La implementación del hipervisor falla y el registro de actividades muestra el siguiente error:

### Acerca de esta tarea

- **Error:** Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""
- **Information:** Successfully deleted drivers from library share sttig.tejasqa.com for <server uuid>
- **Error:** Deleting staging share (drivers) for <server uuid> failed.

Estos errores pueden ocurrir debido a un resultado excepcional del comando `let de VMM GET-SCJOB status` y los archivos del controlador se conservan en el recurso compartido de biblioteca. Antes de volver a intentarlo o de implementar el hipervisor nuevamente, debe eliminar estos archivos del recurso compartido de biblioteca.

Para extraer archivos del recurso compartido de biblioteca:

### Pasos

- 1 En la consola de SCVMM, seleccione **Library (Biblioteca) > Library Servers(Servidores de biblioteca)** y seleccione el servidor de IG que se agregó como servidor de la biblioteca.
- 2 En el servidor de la biblioteca, seleccione y elimine el recurso compartido de la biblioteca.
- 3 Después de eliminar el recurso compartido de biblioteca, conéctese al recurso compartido de IG mediante `\\<Integration Gateway server>\LCDriver\`.
- 4 Elimine la carpeta que contiene los archivos del controlador.

Ahora puede implementar sistemas operativos.

## Error en la implementación del hipervisor en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory

Ocurre un error en la implementación del hipervisor en la 11.ª generación de servidores blade PowerEdge cuando se utilizan las credenciales de usuario de Active Directory. La 11.ª generación de servidores blade PowerEdge usa el protocolo de Interfaz de administración de plataforma inteligente (IPMI) para la comunicación. Sin embargo, la IPMI no es compatible con el uso de credenciales de la configuración de Active Directory.

### Acerca de esta tarea

Para solucionar este problema e implementar sistemas operativos en estos servidores, utilice perfiles de credenciales admitidos.

## Credenciales incorrectas durante la detección

- Si proporciona detalles de credenciales incorrectos durante la detección, en función de la versión de la iDRAC, están disponibles las siguientes soluciones:
    - Al detectar un servidor Dell PowerEdge de 12.<sup>a</sup> generación con la versión de la iDRAC 2.10.10.10 o una versión posterior, si se proporcionan detalles incorrectos del perfil de credenciales, ocurrirá un error en la detección del servidor con el siguiente comportamiento:
      - Para el primer intento, no se bloquea la dirección IP del servidor.
      - Para el segundo intento, se bloquea la dirección IP del servidor durante 30 segundos.
      - Para el tercer intento y para intentos posteriores, se bloquea la dirección IP del servidor durante 60 segundos.
- Puede intentar descubrir el servidor con detalles correctos del perfil de credenciales cuando se desbloquea la dirección IP.
- Al detectar de un servidor PowerEdge de 11.<sup>a</sup> o 12.<sup>a</sup> generación con versiones de iDRAC anteriores a la 2.10.10.10, si los intentos de detección del servidor fallan por haber introducido detalles incorrectos del perfil de credenciales, vuelva a detectar el servidor con los detalles correctos del perfil de credenciales.
  - Para las versiones de la iDRAC anteriores a la 2.10.10.10, el bloqueo de direcciones IP se puede configurar. Para obtener más información, consulte la documentación de la iDRAC en [Dell.com/idracmanuals](http://Dell.com/idracmanuals). En función de sus requisitos, también puede deshabilitar el bloqueo de direcciones IP. También puede verificar si la función **iDRAC.IPBlocking.BlockEnable** está habilitada en la iDRAC.
  - Si el perfil de credenciales predeterminado de la iDRAC se modifica después de detectar un servidor y agregarlo al dispositivo, no se podrá realizar ninguna actividad en el servidor. Para trabajar con el servidor, vuelva a detectarlo con el nuevo perfil de credenciales.

## Problema de instalación de IG mientras se ejecutan varias instancias del instalador en el mismo servidor

Si intenta ejecutar otra instancia de IG después de iniciar la instalación de IG, aparecerá un mensaje de error. Después de hacer clic en Aceptar, se le pedirá que guarde otro archivo MSI de IG.

Para solucionar este problema, no guarde este archivo y continúe con la primera instalación.

## La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas

Después de enviar el trabajo de perfil del servidor de importación al dispositivo, puede que se agote el tiempo de espera pasadas dos horas.

Para solucionar este problema, realice los pasos siguientes:

- 1 Pulse F2 e introduzca la **BIOS Settings (Configuración del BIOS)**.
- 2 Haga clic en **System Setup (Configuración del sistema)** y seleccione **Miscellaneous Settings (Otros ajustes)**.
- 3 Deshabilite **F1/F2 Prompt on Error (Indicador de F1/F2 en caso de error)**.

Después de realizar los pasos siguientes, programe el trabajo de exportación de perfil de servidor y utilice los mismos para completar el trabajo de importación de perfil de servidor correctamente.

## La información de inventario más reciente no aparece incluso después una actualización del firmware

Aunque el trabajo de actualización de firmware se ha completado en un servidor Dell PowerEdge de 11.<sup>a</sup> generación, las versiones de firmware más recientes no aparecen en el inventario del dispositivo.

En el dispositivo, la actualización del inventario es una actividad que se realiza inmediatamente después de completar un trabajo de actualización de firmware. La actualización de firmware finaliza incluso antes de que lo haga la actividad de CSIOR del servidor PowerEdge debido a que información sobre inventario de firmware se muestra antes.

Para solucionar este problema, compruebe si la actividad de CSIOR se completó en el servidor PowerEdge y, luego, actualice el inventario de firmware en el dispositivo. Además, asegúrese de reiniciar el servidor después de aplicar una actualización en etapas sin agente. Para obtener más información sobre cómo actualizar el inventario, consulte [Visualización y actualización del inventario de firmware](#).

Para obtener más información sobre CSIOR, consulte la sección Solución de problemas en la versión más reciente de la *Dell Lifecycle Controller GUI User's Guide* (Guía del usuario de la interfaz gráfica de usuario de Dell Lifecycle Controller) disponible en [dell.com/support/home](https://dell.com/support/home).

## Error 21119 de SCVMM VMM al agregar servidores Active Directory

Al agregar servidores a Active Directory, aparece el error 21119 de SCVMM. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

### Acerca de esta tarea

Para solucionar este problema, realice lo siguiente:

#### Pasos

- 1 Espere para ver si el servidor se ha agregado a Active Directory.
- 2 Si el servidor no se agrega a Active Directory, agregue manualmente los servidores a Active Directory.
- 3 Agregue el servidor a SCVMM.
- 4 Una vez agregado el servidor a SCVMM, vuelva a descubrirlo en la extensión de consola de OMIMSSC para SCVMM.  
El servidor aparecerá en la pestaña **Host**.

# Apéndice

# Acceso a documentos desde el sitio de asistencia de Dell EMC

Puede acceder a los documentos necesarios mediante una de las siguientes formas:

- Para ver documentos de EMC Connections Enterprise Systems Management: [Dell.com/SoftwareSecurityManuals](https://dell.com/softwaresecuritymanuals)
- Para ver documentos de Dell EMC OpenManage: [Dell.com/OpenManageManuals](https://dell.com/openmanagemanuals)
- Para ver documentos de Dell EMC Remote Enterprise Systems Management: [Dell.com/esmanuals](https://dell.com/esmanuals)
- Para ver documentos de iDRAC y Dell EMC Lifecycle Controller: [Dell.com/idracmanuals](https://dell.com/idracmanuals)
- Para ver documentos de EMC OpenManage Connections Enterprise Systems Management: [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://dell.com/OMConnectionsEnterpriseSystemsManagement)
- Para ver documentos de Dell EMC Serviceability Tools: [Dell.com/ServiceabilityTools](https://dell.com/serviceabilitytools)
- Para ver documentos de Client Command Suite Systems Management: [Dell.com/DellClientCommandSuiteManuals](https://dell.com/dellclientcommandsuitemanuals)
- a Vaya a [Dell.com/Support/Home](https://dell.com/support/home).
- b Haga clic en **Choose from all products** (Elegir entre todos los productos).
- c En la sección **All products** (Todos los productos), haga clic en **Software & Security** (Software y seguridad) y, a continuación, haga clic en el vínculo necesario entre los siguientes:
  - **Enterprise Systems Management (Administración de sistemas empresariales)**
  - **Remote Enterprise Systems Management (Administración remota de sistemas empresariales)**
  - **Serviceability Tools (Herramientas de servicio)**
  - **Dell Client Command Suite (Conjunto de comandos del cliente de Dell)**
  - **Connections Client Systems Management (Administración de las conexiones de los sistemas del cliente)**
- d Para ver un documento, haga clic en la versión del producto requerida.
- Mediante los motores de búsqueda:
  - Escriba el nombre y la versión del documento en el cuadro de búsqueda.

## Cómo ponerse en contacto con Dell

### Prerequisito

**NOTA:** Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell.

### Acerca de esta tarea

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

### Pasos

- 1 Vaya a [Dell.com/support](https://dell.com/support).
- 2 Seleccione la categoría de soporte.
- 3 Seleccione su país o región en la lista desplegable **Elija un país o región** que aparece al final de la página.
- 4 Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.