

OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager

Unified User's Guide

Notas, precauciones y advertencias

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

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

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

Chapter 1: Introducción a OMIMSSC OMIMSSC.....	10
Novedades.....	10
Chapter 2: OMIMSSC Componentes.....	11
Chapter 3: Requisitos de sistema para OMIMSSC.....	13
Matriz de compatibilidad.....	13
Privilegios de cuentas.....	15
Requisitos del sistema comunes para OMIMSSC.....	15
Requisitos del sistema de la extensión de la consola de OMIMSSC para SCCM.....	16
Requisitos del sistema de la extensión de la consola de OMIMSSC para SCVMM.....	16
Requisitos de red.....	16
Chapter 4: Implementar OMIMSSC.....	18
Descarga de OMIMSSC en Internet.....	18
Configuración del dispositivo OMIMSSC.....	18
Inscripción de varias consolas de Microsoft.....	19
Inicio del portal de administración de OMIMSSC para descargar los componentes de OMIMSSC.....	20
Instalación de la extensión de la consola de OMIMSSC para SCCM.....	20
Instalación de la extensión de la consola de OMIMSSC para SCVMM.....	20
Chapter 5: Licencia de OMIMSSC.....	21
Opciones que aparecen después de cargar las licencias.....	21
Cumplimiento.....	22
Importación de la licencia en OMIMSSC.....	22
Visualización de información detallada de licencias.....	23
Chapter 6: Inscripción de la consola de Microsoft en OMIMSSC.....	24
Inicio del dispositivo OMIMSSC desde la consola inscrita de Microsoft.....	24
Incorporación de la dirección del FQDN de OMIMSSC en el navegador.....	25
Inicio de la extensión de la consola de OMIMSSC para SCCM.....	25
Inicio de la extensión de la consola de OMIMSSC para SCVMM.....	25
Chapter 7: Cómo administrar OMIMSSC y sus componentes.....	26
Vista de detalles del dispositivo OMIMSSC.....	26
Vista de la administración de usuarios de OMIMSSC.....	26
Visualización o actualización de las consolas inscritas.....	26
Cambio de la contraseña del dispositivo OMIMSSC.....	26
Reparación o modificación de los instaladores.....	27
Reparación de la extensión de la consola de OMIMSSC para SCCM.....	27
Reparación de la extensión de la consola de OMIMSSC para SCVMM.....	27
Modificación de las cuentas de SCCM y SCVMM en el portal de administración del dispositivo OMIMSSC.....	27

Chapter 8: Respaldo y restauración del dispositivo OMIMSSC.....	28
Respaldo del dispositivo OMIMSSC	28
Restaurar dispositivo OMIMSSC.....	28
Restauración del dispositivo OMIMSSC	29
Chapter 9: Desinstalación de OMIMSSC.....	30
Cancelación de la inscripción de la consola de Microsoft en OMIMSSC OMIMSSC.....	30
Desinstalación de la extensión de consola de OMIMSSC para SCCM.....	30
Desinstalación de la extensión de la consola de OMIMSSC para SCVMM.....	31
Quitar la extensión de la consola de OMIMSSC para SCVMM.....	31
Quitar la extensión de la consola de OMIMSSC en SCVMM.....	31
Otros pasos de desinstalación.....	31
Eliminación de cuentas de ejecución específicas del dispositivo.....	31
Eliminación de perfil de aplicación de OMIMSSC.....	31
Eliminación de la máquina virtual del dispositivo.....	31
Chapter 10: Actualización de OMIMSSC para SCVMM.....	32
Acerca de las actualizaciones de Service Pack.....	32
Requisitos previos de instalación.....	33
Instrucciones para actualizar los Service Pack.....	33
Copia de las actualizaciones de Service Pack en el repositorio.....	33
Proporcione información de las direcciones URL del repositorio para las actualizaciones de Service Pack.....	34
Instalación de actualizaciones de Service Pack.....	34
Actualización de la extensión de la consola de OMIMSSC para SCCM.....	35
Actualización de la extensión de la consola de OMIMSSC para SCVMM.....	35
Chapter 11: Reinicio del dispositivo OMIMSSC.....	36
Chapter 12: Cierre de sesión del dispositivo OMIMSSC.....	37
Chapter 13: Administración de perfiles.....	38
Acerca del perfil de credenciales.....	38
Creación de perfil de credenciales.....	38
Modificación de perfil de credenciales.....	39
Eliminación de un perfil de credenciales.....	39
Acerca del perfil de hipervisor (para usuarios de SCVMM).....	40
Creación de perfil de hipervisor.....	40
Modificación de un perfil de hipervisor.....	40
Eliminación de perfil de hipervisor.....	41
Chapter 14: Descubrimiento de dispositivos y sincronización de servidores con la consola de MSSC.....	42
Descubrir dispositivos en OMIMSSC.....	42
Descubrimiento de dispositivos en la extensión de consola de OMIMSSC para SCCM.....	42
Descubrimiento de dispositivos en la extensión de consola de OMIMSSC SCVMM.....	43
Requisitos del sistema para los sistemas administrados.....	43
Descubrimiento de servidores mediante descubrimiento automático.....	43

Descubrir servidores mediante el descubrimiento manual.....	43
Descubrir MX7000 mediante el descubrimiento manual.....	44
Sincronización de extensión de consola de OMIMSSC con SCCM inscrito.....	45
Sincronización de extensión de consola de OMIMSSC con SCVMM inscrito.....	45
Sincronizar con consola Microsoft inscrita.....	45
Resolver errores de sincronización.....	46
Ver el modo de bloqueo del sistema.....	46
Eliminar servidores en OMIMSSC.....	46
Eliminar sistemas modulares en OMIMSSC.....	47
Chapter 15: Vistas en OMIMSSC.....	48
Iniciar vista de servidor.....	48
Iniciar Vista de sistemas modulares.....	49
Iniciar la consola OpenManage Enterprise Modular.....	50
Módulos de entrada/salida.....	50
Iniciar Vista de clúster.....	50
Iniciar la consola iDRAC.....	50
Iniciar el centro de mantenimiento.....	51
Abrir el centro de trabajos y registros.....	51
Chapter 16: Administrar Plantilla operativa.....	53
Plantilla operativa predefinidas.....	54
Acerca de la configuración de un servidor de referencia.....	54
Crear una Plantilla operativa a partir de servidores de referencia.....	54
Componente del SO Windows para la extensión de consola de OMIMSSC para SCCM.....	56
Componente de Windows para la extensión de consola de OMIMSSC para SCVMM.....	56
Componente no perteneciente a Windows para las extensiones de consola de OMIMSSC.....	56
Crear una Plantilla operativa a partir de sistemas modulares de referencia.....	57
Visualizar una Plantilla operativa.....	58
Modificar una Plantilla operativa.....	58
Configurar valores específicos del sistema (valores de pool) mediante una plantilla operativa en varios servidores.....	59
Eliminar una Plantilla operativa.....	59
Asignar una Plantilla operativa y evaluar la compatibilidad de Plantilla operativa para los servidores.....	59
Implementar una Plantilla operativa en servidores.....	60
Asignar una Plantilla operativa a sistemas modulares.....	61
Implementar Plantilla operativa para un sistema modular.....	61
Cancelar asignación de Plantilla operativa.....	62
Acerca de la configuración del sistema modular de referencia.....	62
Chapter 17: Preparación para implementar un sistema operativo.....	63
Acerca de la imagen de WinPE.....	63
Proporcionar un archivo WIM para SCCM.....	63
Proporcionar un archivo WIM para SCVMM.....	63
Extraer controladores de DTK.....	64
Actualizar una imagen de WinPE.....	64
Preparación para implementar el sistema operativo en la consola de SCCM.....	65
Secuencia de tareas en SCCM.....	65
Configuración de una ubicación predeterminada de recurso compartido para el medio de inicio de Lifecycle Controller.....	66

Creación de una ISP de inicio de medio de secuencia de tareas.....	67
Preparación para implementar un sistema operativo distinto a Windows.....	67
Chapter 18: Crear clústeres utilizando una Plantilla operativa.....	68
Crear un switch lógico para clústeres de Storage Spaces Direct.....	68
Creación de clústeres de Storage Spaces Direct.....	68
Chapter 19: Actualización del firmware en OMIMSSC.....	70
Acerca de los grupos de actualización.....	70
Visualización grupos de actualización.....	71
Creación de grupos actualización personalizados.....	71
Modificación de grupos actualización personalizados.....	71
Eliminación de grupos actualización personalizados.....	71
Acerca de los orígenes de actualización.....	72
Configuración de FTP local.....	73
Configuración de HTTP local.....	74
Configuración de HTTPS local.....	74
Visualización del origen de actualizaciones.....	74
Creación de un origen de actualizaciones.....	74
Modificación del origen de actualizaciones.....	75
Eliminación de origen de actualizaciones.....	75
Integración en Dell EMC Repository Manager (DRM).....	76
Integración de DRM con OMIMSSC OMIMSSC.....	76
Establecer la frecuencia de sondeo.....	76
Visualización y actualización del inventario de dispositivos.....	77
Aplicar filtros.....	78
Eliminar filtros.....	78
Actualizar y revertir versiones de firmware mediante el método Ejecutar actualización.....	78
Integración en Dell EMC Repository Manager (DRM).....	79
Chapter 20: Administrar dispositivos en OMIMSSC.....	81
Recuperación de un servidor.....	81
Almacén de protección.....	81
Exportación de perfiles de servidor.....	82
Importar perfil de servidor.....	82
Aplicar ajustes de configuración y firmware en componente de reemplazo.....	83
Recopilar registros de LC para servidores.....	84
Ver registros de LC.....	85
Descripción de archivo.....	85
Exportar inventario.....	86
Cancelar trabajos programados.....	86
Chapter 21: Aprovisionamiento de dispositivos desde OMIMSSC OMIMSSC.....	87
Flujo de trabajo para escenarios de implementación.....	87
Implementación de un sistema operativo Windows mediante la extensión de la consola de OMIMSSC para SCCM.....	88
Implementación de un hipervisor mediante la extensión de la consola de OMIMSSC para SCVMM.....	89
Volver a implementar el sistema operativo Windows mediante OMIMSSC OMIMSSC.....	90

Implementación de un sistema operativo distinto a Windows mediante las extensiones de la consola de OMIMSSC.....	90
Crear clústeres de Storage Spaces Direct mediante Plantilla operativa predefinidas.....	90
Flujo de trabajo para el mantenimiento de dispositivos.....	91
Actualizar el firmware de servidores y dispositivos MX7000.....	91
Configurar los componentes sustituidos.....	93
Exportación e importación de perfiles de servidor.....	93
Chapter 22: Configuración e implementación.....	94
Casos de uso.....	94
Crear Plantillas operativas.....	94
Carpetas del instalador.....	96
Asignar Plantillas operativas.....	96
Implementar Plantillas operativas.....	97
Componente del sistema operativo Windows para la extensión de la consola de OMIMSSC para SCCM.....	97
Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM.....	98
Componente distinto a Windows para la extensión de la consola de OMIMSSC para SCCM/SCVMM.....	98
Descubrimiento en MSSC inscrita.....	98
Importación del perfil del servidor.....	98
Exportar perfil del servidor.....	99
Ver registros de LC.....	99
Recopilar registros de LC.....	99
Sustitución de piezas.....	99
Sondeo y notificación.....	99
Iniciar iDRAC.....	99
Iniciar módulo de entrada/salida.....	100
Resolución de errores de sincronización.....	100
Sincronizar OMIMSSC con consolas Microsoft inscritas.....	100
Asignar e implementar.....	100
Ejecutar actualización.....	100
Implementar un clúster Azure Stack HCI.....	101
Chapter 23: Escenarios de solución de problemas.....	102
Recursos necesarios para administrar OMIMSSC OMIMSSC.....	102
Verificación de los permisos de uso de la extensión de la consola de OMIMSSC para SCCM.....	103
Configuración de acceso de usuario a WMI.....	103
Verificación de los permisos de PowerShell para usar la extensión de la consola de OMIMSSC para SCVMM.....	104
Instalación y actualización de escenarios en OMIMSSC OMIMSSC.....	104
Falla en la inscripción.....	105
Falla en la conexión de prueba.....	105
Falla en la conexión de la extensión de la consola de OMIMSSC para SCVMM.....	105
Error en el acceso a la extensión de la consola después de actualizar SCVMM R2.....	106
La dirección IP no está asignada al dispositivo OMIMSSC.....	106
SCVMM se bloquea durante la importación de la extensión de la consola de OMIMSSC.....	106
Falla en el inicio de sesión en las extensiones de la consola de OMIMSSC.....	106
Bloqueo de SC2012 VMM SP1 durante la actualización.....	106
OMIMSSC Escenarios de portal de administración de OMIMSSC.....	107

Mensaje de error cuando se accede al portal de administración de OMIMSSC con el navegador Mozilla Firefox.....	107
Falla en la muestra del logotipo de Dell EMC en la pantalla del portal de administración de OMIMSSC.....	107
Escenarios de descubrimiento, sincronización e inventario en OMIMSSC OMIMSSC.....	107
Falla en el descubrimiento de servidores.....	107
No se agregaron servidores descubiertos a toda la colección de All Dell Lifecycle Controller Servers.....	107
Falla en el descubrimiento de servidores debido a credenciales incorrectas.....	108
Creación del grupo de chasis VRTX incorrecto después del descubrimiento de servidores.....	108
No se puede sincronizar los servidores host con SCCM inscrito.....	108
No se elimina el grupo de actualización de clúster vacío durante el descubrimiento automático o la sincronización.....	108
Falla en la realización de tareas relacionadas con el mantenimiento en los servidores que se volvieron a descubrir.....	109
Escenarios genéricos en OMIMSSC OMIMSSC.....	109
Falla en el acceso al recurso compartido CIFS con hostname.....	109
Falla en la muestra de la página de trabajos y registros en la extensión de la consola.....	109
Falla de las operaciones en los sistemas administrados.....	109
Falla en el inicio de la ayuda en línea para OMIMSSC.....	109
Escenarios de actualización del firmware en OMIMSSC OMIMSSC.....	110
Error de creación de origen de actualización.....	110
Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema.....	110
Falla en la conexión de prueba del origen local de actualizaciones.....	110
Falla en la creación de un origen de actualización de DRM.....	110
Falla en la creación de un repositorio durante una actualización del firmware.....	110
Error en la muestra del informe de comparación después de actualizar o migrar OMIMSSC.....	111
Falla en la actualización del firmware de los clústeres.....	111
Error de actualización de firmware porque la de cola de trabajos está llena.....	111
Falla en la actualización del firmware con un origen de actualización de DRM.....	112
Actualización del firmware en componentes independientemente de la selección.....	112
Falla en la muestra de información de inventario más reciente después de actualizar el firmware.....	112
Error al eliminar un grupo de actualización personalizado.....	112
Falla en la actualización de la imagen de WinPE.....	113
Cambio del color de la campana para el sondeo y la notificación después de actualizar la frecuencia.....	113
Escenarios de implementación del sistema operativo en OMIMSSC.....	113
Escenarios genéricos de implementación del sistema operativo.....	113
Escenarios de implementación del sistema operativo para los usuarios de SCCM.....	114
Escenarios de implementación del sistema operativo para los usuarios de SCVMM.....	114
Escenarios de creación de clústeres S2D para usuarios de SCVMM.....	115
Escenarios de perfil del servidor en OMIMSSC.....	116
Error al exportar perfiles de servidores.....	116
La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas.....	116
Escenarios de registros de LC en OMIMSSC.....	116
Falla en la exportación de registros de LC en formato .CSV.....	116
Falla en la apertura de los archivos de registro de LC.....	116
Falla en la conexión de prueba.....	117
Chapter 24: Apéndice.....	118

Chapter 25: Apéndice 2.....	121
Chapter 26: Acceso a documentos desde el sitio de asistencia de Dell EMC.....	122

Introducción a OMIMSSC OMIMSSC

Este documento es una guía del usuario unificada que contiene toda la información relacionada con el uso, la instalación y las prácticas recomendadas de OMIMSSC.

OpenManage Integration para Microsoft System Center OpenManage Integration para Microsoft System Center (OMIMSSC) es una integración basada en dispositivos a un conjunto de productos de System Center. OMIMSSC OMIMSSC permite lograr una administración del ciclo de vida completo de los servidores Dell EMC PowerEdge mediante Integrated Dell Remote Access Controller (iDRAC) con Lifecycle Controller (LC).

OMIMSSC OMIMSSC ofrece implementación del sistema operativo, creación de clústeres con Storage Spaces Direct, parches para hardware, actualización de firmware, y mantenimiento de servidores y sistemas modulares. Integre OMIMSSC en Microsoft System Center Configuration Manager (SCCM) para administrar servidores Dell PowerEdge en centros de datos tradicionales, integre OMIMSSC en Microsoft System Center Virtual Machine Manager (SCVMM) para administrar servidores Dell PowerEdge en entornos virtuales y de nube.

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

NOTA: La versión 6.4 de Dell EMC Deployment Tool Kit (DTK) asociada está disponible para los servidores PowerEdge basados en iDRAC9 X5 más recientes, que se utilizarán únicamente con el paquete de OMIMSSC.

NOTA: El DTK es el producto final del ciclo de vida de Dell EMC. Esta versión de DTK solo se admite para su uso con OMIMSSC versión 7.2.1.

Temas:

- [Novedades](#)

Novedades

- Compatibilidad con System Center Configuration Manager (SCCM) versión 1910.
- Compatibilidad con System Center Configuration Manager (SCCM) versión 2002.
- Compatibilidad con System Center Virtual Machine Manager (SCVMM) 2016 UR8.
- Compatibilidad con System Center Virtual Machine Manager (SCVMM) 2016 UR9.
- Compatibilidad con System Center Virtual Machine Manager (SCVMM) 2019 UR1.
- Documento de usuario simplificado. (La Guía de instalación, la Guía del usuario y la información sobre la solución de problemas consolidadas en un único documento unificado).
- Tamaño de archivo del instalador reducido para admitir la descarga más rápida del dispositivo.
- Se implementaron correcciones de seguridad para la autenticación incorrecta, la divulgación de información para los registros del dispositivo y el uso de las vulnerabilidades de clave criptográfica codificadas por hardware. Para obtener más información sobre las correcciones de seguridad, consulte <https://www.dell.com/support/security>.
- Compatibilidad con los servidores PowerEdge basados en iDRAC 9 más recientes.

OMIMSSC Componentes

A continuación, se muestra la lista de los componentes de OMIMSSC y los nombres que se utilizaron en esta guía:

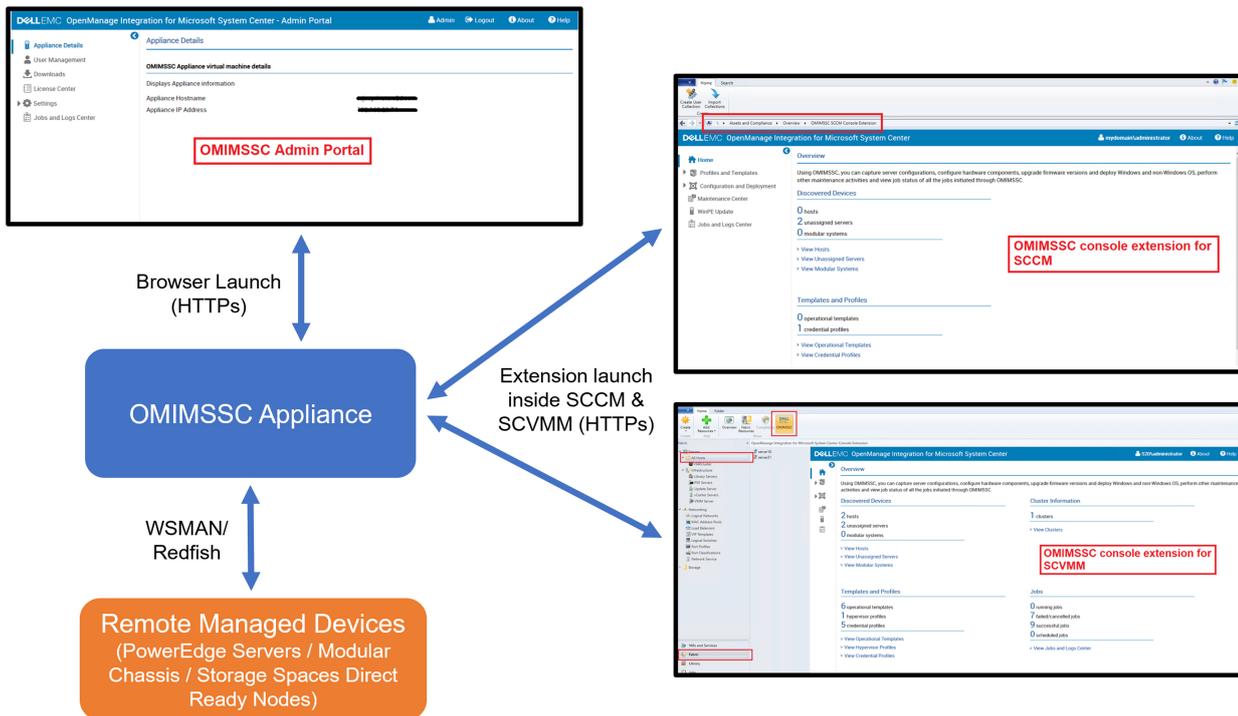
Tabla 1. Componentes en OMIMSSC OMIMSSC

Componentes	Descripción
OpenManage Integration para Microsoft System Center Máquina virtual del dispositivo OpenManage Integration para Microsoft System Center, también conocida como dispositivo OMIMSSC.	<p>Aloja el dispositivo OMIMSSC en una Hyper-V como máquina virtual según CentOS y realiza las siguientes tareas:</p> <ul style="list-style-type: none"> ● Interactúa con los servidores de Dell EMC a través del iDRAC. Para ello, utiliza comandos de Web Services-Management (WSMan). ● Interactúa con los dispositivos Dell EMC PowerEdge MX7000 a través de OpenManage Enterprise Modular (OME-Modular). Para ello, utiliza comandos API REST. ● Le permite administrar el dispositivo OMIMSSC a través del portal de administración de OMIMSSC.
OpenManage Integration para Microsoft System Center Consola de OpenManage Integration para Microsoft System Center, también conocida como la consola de OMIMSSC.	<p>Se utiliza la misma extensión en las consolas de SCCM y SCVMM. También se conoce como:</p> <ul style="list-style-type: none"> ● OMIMSSC Extensión de la consola de OMIMSSC para SCCM ● OMIMSSC Extensión de la consola de OMIMSSC para SCVMM

Los sistemas de administración son los sistemas en los que se instalan OMIMSSC y sus componentes.

Los sistemas administrados son los servidores que OMIMSSC administra.

Arquitectura de OMIMSSC



Requisitos de sistema para OMIMSSC

Temas:

- [Matriz de compatibilidad](#)
- [Privilegios de cuentas](#)
- [Requisitos del sistema comunes para OMIMSSC](#)
- [Requisitos del sistema de la extensión de la consola de OMIMSSC para SCCM](#)
- [Requisitos del sistema de la extensión de la consola de OMIMSSC para SCVMM](#)
- [Requisitos de red](#)

Matriz de compatibilidad

Todas las matrices de soporte disponibles para OMIMSSC son las siguientes:

OMIMSSC System Center compatible con OMIMSSC

- Microsoft System Center Configuration Manager (SCCM) 2012 SP1
- Microsoft System Center Configuration Manager (SCCM) 2012 SP2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2 SP1
- Microsoft System Center Configuration Manager (SCCM) 1610
- Microsoft System Center Configuration Manager (SCCM) versión 1809
- Microsoft System Center Configuration Manager (SCCM) versión 1810
- Microsoft System Center Configuration Manager (SCCM) versión 1902
- Microsoft System Center Configuration Manager (SCCM) versión 1906
- Microsoft System Center Configuration Manager (SCCM) versión 1910
- Microsoft System Center Configuration Manager (SCCM) versión 2002
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 SP1
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR8
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR9
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR1
- Microsoft System Center Virtual Machine Manager (SCVMM) SAC versión 1807

Tabla 2. Dispositivos compatibles

Dell EMC System	Versión compatible
Servidores PowerEdge basados en iDRAC 9	<ul style="list-style-type: none"> • Paquete de controladores del SO para las plataformas AMD compatibles: <ul style="list-style-type: none"> ○ R6515, R7515, C6525 y R6525: 19.12.08 ○ R7525: 19.12.07 • Versión de Lifecycle Controller y versión de Integrated Dell EMC Remote Access Controller para las plataformas AMD compatibles: <p>SCCM</p> <ul style="list-style-type: none"> ○ R6515 y R7515: 3.40.40.40 o posterior ○ C6525 y R6525: 3.42.42.42 o posterior ○ R7525: 4.10.10.10 o posterior

Tabla 2. Dispositivos compatibles (continuación)

Dell EMC System	Versión compatible
	<p>SCVMM</p> <ul style="list-style-type: none"> ○ R6515, R7515, C6525, R6525 y R7525: 4.30.30.30 o posteriores ● Dell EMC OpenManage Deployment Tool kit versión: 6.4 <p>i NOTA: La implementación del sistema operativo para ESXi no es compatible.</p> <p>i NOTA: La implementación del sistema operativo con el método de inicio en vFlash \ colocación en vFlash y las funciones de respaldo del perfil del servidor no es compatible.</p>
Servidores PowerEdge de 14.ª generación	<ul style="list-style-type: none"> ● Paquete de controladores del SO: 17.05.21 ● Lifecycle Controller versión: 3.00.00.00 o posterior ● Integration Dell EMC Remote Access Controller versión: 3.00.00.00 o posterior ● Dell EMC OpenManage Deployment Tool kit versión: 6.3
Servidores PowerEdge de 13.ª generación	<ul style="list-style-type: none"> ● Paquete de controladores del SO: 16.08.13 ● Lifecycle Controller versión: 2.40.40.40 o posterior ● Integrated Dell Remote Access Controller versión: 2.40.40.40 o posterior ● Dell EMC OpenManage Deployment Tool kit versión: 6.3
Servidores PowerEdge de 12.ª generación	<ul style="list-style-type: none"> ● Paquete de controladores del SO: para los servidores R220 y FM120: 16.08.13 ● Otro paquete de controladores del SO de plataformas compatibles: 15.07.07 ● Lifecycle Controller versión 2.40.40.40 o posterior ● Integration Dell Remote Access Controller versión 2.40.40.40 o posterior ● Dell OpenManage Deployment Tool kit versión: 6.3
Chassis Management Console (CMC)	<ul style="list-style-type: none"> ● FX2 1.4 o posterior ● M1000e 5.2 o posterior ● VRTX 2.2 o posterior
Dell EMC OpenManage Enterprise-Modular	<ul style="list-style-type: none"> ● PowerEdge MX7000 Chassis 1.0

i **NOTA:** La compatibilidad con los servidores PowerEdge de 11.ª generación quedó obsoleta desde la versión 7.2.1 de OMIMSSC en adelante.

Tabla 3. Sistemas operativos compatibles (implementación):

Sistemas operativos	Versión compatible
Microsoft Windows	<ul style="list-style-type: none"> ● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2 ● Windows Server 2012 SP1
Sistema operativo LINUX	<ul style="list-style-type: none"> ● RHEL 7.3, 7.4, 7.5 ● RHEL 7.2 ● RHEL 6.9
VMWare ESXi	<ul style="list-style-type: none"> ● ESXi 6.0 - A02 ● ESXi 6.0 U3 - A15 ● ESXi 6.5 - A03 ● ESXi 6.5 U1 - A11

Tabla 3. Sistemas operativos compatibles (implementación): (continuación)

Sistemas operativos	Versión compatible
	<ul style="list-style-type: none"> ESXi 6.7 - A06 <p> NOTA: Descargue la imagen desde https://www.dell.com/support/, consulte la página Controladores y descargas del modelo de servidor específico de acuerdo con las versiones compatibles con OMIMSSC.</p>

OMIMSSC Clústeres compatibles con OMIMSSC

- Creación y administración de clústeres de Windows 2016 y 2019 S2D habilitados en la consola de SCVMM
- Administración de clústeres de host Hyper-V de Windows 2012 R2, 2016 y 2019 en la consola de SCVMM

Privilegios de cuentas

Todos los privilegios de cuentas requeridos que se deben utilizar en OMIMSSC son los siguientes:

Los privilegios de cuentas para la extensión de la consola de OMIMSSC para SCCM son que el usuario sea un miembro de los siguientes grupos en SCCM:

Tabla 4. Cuentas de usuario con privilegios obligatorios

Usuarios	Privilegios/funciones
para la inscripción	<ul style="list-style-type: none"> La cuenta utilizada para inscribir la consola de SCCM en OMIMSSC debe ser de un administrador con todos los permisos o un administrador en SCCM. La cuenta utilizada para inscribir la consola de SCVMM en OMIMSSC debe ser de un miembro del rol Administrador en SCVMM. Usuario del dominio. Miembro del grupo de administradores locales en System Center Machine.
para iniciar sesión en las extensiones de la consola	<ul style="list-style-type: none"> La cuenta utilizada para inscribir la consola de SCCM en OMIMSSC debe ser de un administrador con todos los permisos o un administrador en SCCM. La cuenta utilizada para inscribir la consola de SCVMM en OMIMSSC debe ser de un administrador delegado o un administrador en SCVMM. Usuario del dominio. Miembro del grupo de administradores locales en System Center Machine.

Requisitos del sistema comunes para OMIMSSC

Antes de instalar OMIMSSC, asegúrese de completar los siguientes requisitos previos de la instalación de software según los tres componentes indicados de OMIMSSC:

- Dispositivo OMIMSSC:
 - Instale Windows Server y habilite la función Hyper-V.
 - Ya puede inscribir la cantidad que desee de consolas de SCCM o SCVMM en un dispositivo OMIMSSC, ya que OMIMSSC admite la inscripción en múltiples consolas. Según la cantidad de consolas que planee inscribir, le presentamos los siguientes requisitos de hardware:

Tabla 5. Requisitos de hardware

Componentes	Para una consola de SCCM o SCVMM	Para una cantidad determinada de consolas de SCCM o SCVMM
RAM	8 GB	8 GB por cantidad de consolas

Tabla 5. Requisitos de hardware (continuación)

Componentes	Para una consola de SCCM o SCVMM	Para una cantidad determinada de consolas de SCCM o SCVMM
Recuento de procesadores	4	4 por cantidad de consolas

- Instale una de las siguientes versiones del sistema operativo de Windows:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

- Portal de administración de OMIMSSC:

Instale cualquiera de los siguientes navegadores web:

- Internet Explorer 10 o posterior
- Mozilla Firefox 30 o posterior
- Google Chrome 23 o posterior
- Microsoft Edge

Para seguir requisitos del sistema específicos de OMIMSSC, ahora puede seguir los requisitos que se mencionan en siguiente vínculo de acuerdo con la consola que utilice:

- [Requisitos del sistema de la extensión de la consola de OMIMSSC para SCCM](#)
- [Requisitos del sistema de la extensión de la consola de OMIMSSC para SCVMM](#)

Requisitos del sistema de la extensión de la consola de OMIMSSC para SCCM

Para instalar la extensión de la consola de OMIMSSC para SCCM, realice los siguientes pasos:

- Instale las mismas versiones de consola de administración y de servidor de sitio de SCCM.

Requisitos del sistema de la extensión de la consola de OMIMSSC para SCVMM

Para instalar la extensión de la consola de OMIMSSC para SCVMM, realice los siguientes pasos:

- Instale las mismas versiones de consola de administración y de servidor de SCVMM.
- La función Clúster de conmutación por error está activada en el servidor SCVMM.
- El usuario inscrito debe tener derechos de administrador en el servidor SCVMM.
- El usuario inscrito debe tener derechos de administrador en el clúster administrado.

Requisitos de red

Los puertos utilizados en OMIMSSC son los siguientes:

Diversos componentes de OMIMSSC utilizan la siguiente lista de puertos y, por lo tanto, debe incluir estos puertos en la lista de excepción de firewall:

Tabla 6. Información sobre los puertos

Uso	Protocolo	Número de puerto
Comunicación iDRAC	WSMan	-
Sistemas modulares	REST	-
Autodiscovery	HTTPS	-

Tabla 6. Información sobre los puertos (continuación)

Uso	Protocolo	Número de puerto
iDRAC: estos puertos están activados para que el iDRAC acceda al recurso compartido de CIFS que el instalador o los usuarios crearon.	HTTPS	135 a 139 y 445

Implementar OMIMSSC

Temas:

- [Descarga de OMIMSSC en Internet](#)
- [Configuración del dispositivo OMIMSSC](#)
- [Inscripción de varias consolas de Microsoft](#)
- [Inicio del portal de administración de OMIMSSC para descargar los componentes de OMIMSSC](#)

Descarga de OMIMSSC en Internet

Para descargar OMIMSSC desde <https://www.dell.com/support>, realice los siguientes pasos:

1. Haga clic en **Examinar todos los productos > Software > Enterprise Systems Management > OpenManage Integration para Microsoft System**.
2. Seleccione la versión requerida de OMIMSSC.
3. Haga clic en la pestaña **Controladores y descargas**.
4. Descargue el archivo VHD de OMIMSSC.
5. Extraiga el archivo VHD y, a continuación, [configure el dispositivo OMIMSSC](#). El tamaño del archivo VHD será de aproximadamente 5 GB, por lo tanto, la implementación tardará entre cinco y diez minutos en completarse.
6. Especifique la ubicación para descomprimir los archivos y haga clic en el botón unzip para extraer los archivos:
 - **OMIMSSC_v7.2.1.2610_for_VMM_and_ConfigMgr**
 - **DellEMC_OpenManage_Deployment_Toolkit_Windows_6.4.0**

 **NOTA:** El DTK versión 6.4 solo se admite para su uso con OMIMSSC versión 7.2.1.

Configuración del dispositivo OMIMSSC

Asegúrese de cumplir los siguientes requisitos en Hyper-V cuando configure el dispositivo OMIMSSC:

- El conmutador virtual está configurado y disponible.
- Asigne memoria a la VM del dispositivo OMIMSSC según la cantidad de consolas de Microsoft que planea inscribir. Para obtener más información, consulte los [Requisitos comunes](#).

Para configurar el dispositivo OMIMSSC:

1. Realice los siguientes pasos para implementar la VM del dispositivo OMIMSSC:
 - a. En **Windows Server** del **Administrador de Hyper-V**, en el menú **Acciones**, seleccione **Nuevo** y haga clic en **Administrador de máquina virtual**. Se muestra el **Asistente de nueva máquina virtual**.
 - b. En **Antes de comenzar**, haga clic en **Siguiente**.
 - c. En **Especificar nombre y ubicación**, proporcione un nombre para la máquina virtual. Si desea almacenar la VM en una ubicación diferente, seleccione **Almacenar la máquina virtual en una ubicación diferente**, haga clic en **Examinar** y acceda a la nueva ubicación.
 - d. En **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.
 - e. En **Asignar memoria**, asigne la capacidad de memoria mencionada en el requisito previo.
 - f. En **Configurar redes**, en **Conexión**, seleccione la red que desee utilizar y, a continuación, haga clic en **Siguiente**.
 - g. En **Conectar disco duro virtual**, seleccione **Usar un disco duro virtual existente**, acceda a la ubicación donde se encuentra el archivo VHD **OMIMSSC_v7.2.1_for_VMM_and_ConfigMgr** y seleccione el archivo. El tamaño del archivo VHD será de aproximadamente 5 GB, por lo tanto, la implementación tardará entre cinco y diez minutos en completarse.

- h. En **Resumen**, confirme los detalles proporcionados y haga clic en **Terminar**.
- i. Establezca en 4 el valor de la **Cantidad de procesadores virtuales**, debido a que, de manera predeterminada, el conteo del procesador está establecido en 1.

Para establecer el conteo del procesador:

- i. Haga clic con el botón secundario en el dispositivo OMIMSSC y seleccione **Configuración**.
- ii. En **Configuración**, seleccione **Procesador** y establezca la **Cantidad de procesadores virtuales** en 4.

2. Inicie la VM del dispositivo OMIMSSC para llevar a cabo las siguientes tareas:
3. Realice las siguientes tareas una vez que se inicie el dispositivo OMIMSSC:

NOTA: Se recomienda que espere cinco minutos antes de iniciar sesión como **Administrador** para que se inicien todos los servicios.

- a. En **Iniciar sesión de host local**: escriba admin.
- b. En **Ingresar nueva contraseña de administrador**: escriba una contraseña.
NOTA: Dell EMC recomienda configurar y usar contraseñas seguras para autenticar al usuario admin del dispositivo y la extensión de la consola.
- c. En **Confirmar nueva contraseña de administrador**: vuelva a escribir la contraseña y, a continuación, pulse **Intro** para continuar.
- d. En las opciones, seleccione **Configurar red**, presione **Intro** y realice los siguientes subpasos:
 - En **NetworkManagerTUI**, seleccione **Establecer hostname del sistema**, proporcione el nombre del dispositivo OMIMSSC y haga clic en **Aceptar**.

Por ejemplo, `Hostname.domain.com`

NOTA: Puede cambiar la dirección IP del dispositivo OMIMSSC si selecciona la opción **Configurar red**. No puede cambiar la dirección IP ni el nombre de host del dispositivo OMIMSSC después de este paso.

- Si proporcionará una dirección IP estática, seleccione **Editar una conexión** y, a continuación, **Ethernet0**. Seleccione **CONFIGURACIÓN DE IPv4**, luego seleccione **Manual** y haga clic en **Mostrar**. Proporcione la dirección de configuración de IP, una puerta de enlace, una dirección IP del servidor DNS y, a continuación, haga clic en **Aceptar**.

- e. Observe la dirección URL del portal de administración de OMIMSSC del dispositivo OMIMSSC.

NOTA: Agregue la dirección IP y el FQDN del dispositivo OMIMSSC en Zonas de búsqueda directa y Zonas de búsqueda inversa en DNS.

NOTA: Los usuarios que no son administradores pueden acceder a los registros del dispositivo. Sin embargo, estos registros no conllevan información confidencial. Como solución alternativa, proteja la URL del dispositivo.

Inscripción de varias consolas de Microsoft

Administre los recursos de un dispositivo OMIMSSC cuando haya varias consolas de Microsoft inscritas en OMIMSSC.

Según la cantidad de consolas de Microsoft que desee inscribir en el dispositivo OMIMSSC, asegúrese de satisfacer los requisitos del hardware. Para obtener más información, consulte [Requisitos comunes del sistema para OMIMSSC](#).

Para configurar los recursos para varias consolas de Microsoft, realice los siguientes pasos:

1. Inicie el dispositivo OMIMSSC e inicie sesión en él.
2. Navegue hasta **Configurar parámetros de inscripción** y haga clic en **Ingresar**.
3. Proporcione la cantidad de consolas que desea inscribir en el dispositivo OMIMSSC. Se incluyen los recursos necesarios.

Inicio del portal de administración de OMIMSSC para descargar los componentes de OMIMSSC

1. Inicie el navegador e inicie sesión en el portal de administración de OMIMSSC con las mismas credenciales que usó cuando inició sesión en el dispositivo OMIMSSC

Formato: `https://<IP address or FQDN>`

 **NOTA:** Agregue la dirección URL del portal de administración de OMIMSSC en el **Sitio de intranet local**. Para obtener más información, consulte [Agregar dirección IP de OMIMSSC en el navegador](#).

2. Haga clic en **Descargas** y en **Descargar instalador** para descargar la extensión de la consola.

Instalación de la extensión de la consola de OMIMSSC para SCCM

- Asegúrese de instalar el dispositivo OMIMSSC en el servidor de sitio de SCCM antes de usarlo en la consola de administración de SCCM.
 - Se recomienda cerrar Configuration Manager antes de instalar, actualizar o desinstalar la extensión de la consola de OMIMSSC para SCCM.
1. Haga doble clic en `OMIMSSC_SCCM_Console_Extension.exe`. Se muestra la pantalla de **bienvenida**.
 2. Haga clic en **Siguiente**.
 3. En la pantalla **Contrato de licencia**, seleccione **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
 4. En la página **Carpeta de destino**, hay una carpeta de instalación seleccionada de manera predeterminada. Para cambiar la ubicación, haga clic en **Cambiar**, acceda a una nueva ubicación y, a continuación, haga clic en **Siguiente**.
 5. En la página **Preparado para instalar el programa**, haga clic en **Instalar**. Se crea la siguiente carpeta después de instalar la extensión de la consola:
 - Registro: esta carpeta contiene información de registro relacionada con la consola.
 6. En **La instalación finalizó correctamente**, haga clic en **Terminar**.

Instalación de la extensión de la consola de OMIMSSC para SCVMM

- Instale la extensión de la consola de OMIMSSC en el servidor de administración y en la consola SCVMM. Solamente después de instalar la consola de OMIMSSC puede importar la extensión de la consola a SCVMM.
1. Haga doble clic en `OMIMSSC_SCVMM_Console_Extension.exe`. Se muestra la pantalla de **bienvenida**.
 2. Haga clic en **Siguiente**.
 3. En la pantalla **Contrato de licencia**, seleccione **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
 4. En la página **Carpeta de destino**, hay una carpeta de instalación seleccionada de manera predeterminada. Para cambiar la ubicación, haga clic en **Cambiar**, acceda a una nueva ubicación y, a continuación, haga clic en **Siguiente**.
 5. En la página **Preparado para instalar el programa**, haga clic en **Instalar**. Las siguientes carpetas se crean después de instalar la extensión de consola:
 - Registro: esta carpeta contiene información de registro relacionada con la consola.
 - OMIMSSC_UPDATE—: esta carpeta se compone de todas las actividades requeridas para la actualización compatible con clústeres (CAU, por sus siglas en inglés). Esta carpeta tiene permisos de lectura y escritura solamente para las operaciones de CAU. Los permisos del Instrumental de administración de Windows (WMI, por sus siglas en inglés) se configuran para esta carpeta. Para obtener más información, consulte la documentación de Microsoft.
 6. En la página **Asistente InstallShield completado**, haga clic en **Terminar**.
 7. Importe la extensión de la consola de OMIMSSC para SCVMM en la consola SCVMM. Para obtener más información, consulte [Importación de la extensión de la consola de OMIMSSC para SCVMM](#).

Licencia 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), la que se importa automáticamente después de la instalación. Esto solamente corresponde para los servidores de 11.ª generación y generaciones posteriores de los servidores de Dell EMC.
- Licencia de producción: puede adquirir una licencia de producción de Dell EMC para la cantidad de servidores que OMIMSSC administrará. Esta licencia incluye el soporte del producto y las actualizaciones para el dispositivo OMIMSSC.

Cuando compra una licencia, el archivo .XML (clave de licencia) se encuentra disponible para su descarga en Dell Digital Locker. Si no puede descargar sus claves de licencia, comuníquese con el Soporte de Dell en dell.com/support/softwarecontacts a fin de ubicar el número telefónico del Soporte de Dell regional 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, se libera una licencia. Se crea una entrada en el registro de actividades de OMIMSSC en el caso de las siguientes actividades:

- Se importa un archivo de licencia.
- Se elimina el servidor de OMIMSSC y se renuncia a la licencia.
- Se consume la licencia después de detectar un servidor.

Después de pasar de una licencia de evaluación a una de producción, se sobrescribe la licencia de evaluación con la de producción. La cantidad de **nodos con licencia** es igual a la cantidad de licencias de producción adquiridas.

Temas:

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

Opciones que aparecen después de cargar las licencias

A continuación, se muestran las opciones compatibles con la función de licencia en OMIMSSC

Archivo de licencia para nuevas compras realizadas

Cuando realiza un pedido para adquirir una licencia nueva, se envía un correo electrónico desde Dell con la confirmación del pedido y, a continuación, puede descargar el archivo nuevo de licencia desde Dell Digital Store. La licencia se encuentra en formato .xml. Si la licencia está en formato zip, extraiga el archivo de licencia .xml desde el archivo zip antes de cargarlo.

Apilamiento de licencias

Puede apilar varias licencias de producción para aumentar la cantidad de servidores compatibles a la suma de servidores en las licencias cargadas. No se puede apilar una licencia de evaluación. La cantidad de servidores compatibles no se podrá aumentar con el apilamiento y se requiere del uso de varios dispositivos OMIMSSC.

Si ya hay varias licencias cargadas, la cantidad de servidores compatibles es 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 cuando intente cargar un archivo modificado o dañado, se mostrará un mensaje de error. Puede solicitar otro archivo de licencia en Dell Digital Locker. Cuando reciba una licencia de reemplazo, esta contendrá el mismo ID de autorización de la licencia anterior. Cuando cargue una licencia de reemplazo, se reemplazará la licencia si ya cargó una con el mismo ID de autorización.

Reimportación de licencias

Si intenta importar el mismo archivo de licencia, se mostrará un mensaje de error. Adquiera una licencia nueva e importe el archivo nuevo de licencia.

Importación de varias licencias

Puede importar varios archivos de licencia con diferentes ID de autorización para aumentar la cantidad de servidores de detección y mantenimiento 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 la licencia en OMIMSSC

Tras la compra de una licencia, impórtela a OMIMSSC. Para ello, realice los pasos siguientes:

1. En el portal de administración de OMIMSSC, haga clic en **Centro de licencias**.
2. Haga clic en **Importar licencia** y seleccione el archivo de licencia descargado desde Dell Digital Store.

NOTA: Solamente puede importar archivos de licencia válidos. Si el archivo está dañado o manipulado, se mostrará un mensaje de error según corresponda. Descargue el archivo nuevamente desde Dell Digital Store o comuníquese 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.

Inscripción de la consola de Microsoft en OMIMSSC

- Para los usuarios de SCCM, se instala la extensión de la consola de OMIMSSC para la consola SCCM.
- Para los usuarios de SCVMM, se instala la extensión de la consola de OMIMSSC para SCVMM.

Asegúrese de que la siguiente información está disponible:

- La información de identificación del sistema en el que está configurado Microsoft, consulte los [privilegios de cuentas necesarios](#).
- El FQDN de SCCM o el FQDN de SCVMM.

Realice los siguientes pasos para inscribir una consola de SCCM o SCVMM en OMIMSSC:

1. Abra un navegador y proporcione la dirección URL del dispositivo OMIMSSC.
Aparece la página de inicio de sesión del portal de administración de OMIMSSC.
2. Haga clic en **Configuración**, en **Inscripción de consolas** y, a continuación, en **Inscribir**.
Aparece la página **Inscribir una consola**.
3. Ingrese un nombre y una descripción para la consola.
4. Proporcione el FQDN del servidor de sitio de SCCM, o servidor SCVMM, y las credenciales.
5. (Opcional) Haga clic en **Crear nuevo** para crear un perfil de credencial tipo Windows a fin de acceder a la consola de SCCM o SCVMM.
 - Seleccione el **Tipo de perfil de credencial** como **Perfil de credencial de Windows**.
 - Escriba un nombre y una descripción del perfil.
 - En **Credenciales**, escriba el nombre de usuario y la contraseña.
 - Proporcione los detalles del dominio en **Dominio**.

NOTA: Cuando cree el perfil de credencial para la inscripción de consola, escriba el nombre de dominio con detalles de Dominio de nivel superior (TLD).

Por ejemplo, si el nombre de dominio es `mydomain` y el TLD es `com`, escriba el nombre de dominio en el perfil de credencial como: `mydomain.com`.

6. Para verificar las conexiones entre el dispositivo OMIMSSC y la consola de Microsoft, haga clic en **Probar conexión**.
7. Para inscribir la consola luego de una prueba de conexión correcta, haga clic en **Inscribir**.

NOTA: Después de la inscripción, OMIMSSC crea una cuenta en SCVMM con el nombre **Perfil de registro de la extensión de la consola SCVMM de OMIMSSC**. Asegúrese de no borrar este perfil, ya que no podrá ejecutar ninguna operación en OMIMSSC si lo hace.

NOTA: Inscriba el servidor de sitio de SCCM para utilizar la extensión de la consola de OMIMSSC en la consola de administración de SCCM.

Temas:

- [Inicio del dispositivo OMIMSSC desde la consola inscrita de Microsoft](#)

Inicio del dispositivo OMIMSSC desde la consola inscrita de Microsoft

Inicie el dispositivo OMIMSSC desde una consola inscrita de SCCM o SCVMM.

Incorporación de la dirección del FQDN de OMIMSSC en el navegador

Antes de iniciar el dispositivo OMIMSSC, agregue la dirección FQDN de OMIMSSC como un requisito previo en la lista de sitios de la **Intranet local**. Para ello, realice los pasos siguientes:

1. Haga clic en **Configuración de IE** y, a continuación, en **Opciones de Internet**.
2. Haga clic en **Configuración avanzada** y, en **Configuración**, busque la sección **Seguridad**.
3. Desmarque la opción **No guardar las páginas cifradas en el disco** y haga clic en **Aceptar**.

Inicio de la extensión de la consola de OMIMSSC para SCCM

Vea la tabla de privilegios de usuario que se menciona en los [privilegios de cuentas](#).

En la consola de SCCM, haga clic en **Activos y cumplimiento de normas**, en **Descripción general** y, a continuación, en **Extensión de la consola de OMIMSSC para SCCM**.

NOTA: Si se conecta a la consola de SCCM mediante el Protocolo de escritorio remoto (RDP, por sus siglas en inglés) y, a continuación, cierra ese protocolo, es posible que se cierre la sesión en el dispositivo OMIMSSC. Por lo tanto, inicie sesión después de volver a abrir la sesión de RDP.

Inicio de la extensión de la consola de OMIMSSC para SCVMM

Para iniciar la extensión de la consola de OMIMSSC para SCVMM, realice los siguientes pasos:

1. Importe la extensión de la consola a SCVMM. Para obtener más información, consulte [Importación de la extensión de la consola de OMIMSSC para SCVMM](#).
2. Inicie la extensión de la consola en SCVMM. Para obtener más información, consulte [Inicio de la extensión de la consola de OMIMSSC desde SCVMM](#).

Importación de la extensión de la consola de OMIMSSC para SCVMM

Para importar la extensión de la consola de OMIMSSC para SCVMM, realice los siguientes pasos:

1. Inicie la consola de SCVMM con privilegios de administrador o como administrador delegado.
2. Haga clic en **Configuración** y, a continuación, haga clic en **Importar complemento de consola**. Aparece el **Asistente de importación del complemento de consola**.
3. Haga clic en **Examinar** y seleccione el archivo zip desde `C:\Archivos de programa\OMIMSSC\VMM Console Extension`, haga clic en **Siguiente** y en **Finalizar**. Asegúrese de que el complemento es válido.

Inicio de la extensión de la consola de OMIMSSC para SCVMM

1. En la consola de SCVMM, seleccione **Fabric** y, a continuación, seleccione los grupos de servidores para **Todos los hosts**.

NOTA: Para iniciar la consola de OMIMSSC, puede seleccionar cualquier grupo de hosts al que tenga permisos de acceso.

2. En barra de **Página de inicio**, seleccione **DELL EMC OMIMSSC**.

Cómo administrar OMIMSSC y sus componentes

Temas:

- Vista de detalles del dispositivo OMIMSSC
- Vista de la administración de usuarios de OMIMSSC
- Visualización o actualización de las consolas inscritas
- Cambio de la contraseña del dispositivo OMIMSSC
- Reparación o modificación de los instaladores
- Modificación de las cuentas de SCCM y SCVMM en el portal de administración del dispositivo OMIMSSC

Vista de detalles del dispositivo OMIMSSC

1. Inicie el portal del administrador de OMIMSSC desde un navegador.
2. Inicie sesión en el portal de administración de OMIMSSC mediante las mismas credenciales que se utilizaron para iniciar sesión en la VM del dispositivo OMIMSSC y, a continuación, haga clic en **Detalles del dispositivo**. Se muestra la dirección IP y el nombre de host del dispositivo OMIMSSC.

Vista de la administración de usuarios de OMIMSSC

1. Inicie el portal del administrador de OMIMSSC desde un navegador.
2. Inicie sesión en el portal de administración de OMIMSSC mediante las mismas credenciales que se utilizaron para iniciar sesión en la VM del dispositivo OMIMSSC y, a continuación, haga clic en **Administración de usuarios de OMIMSSC**. Se mostrará el estado de los usuarios que se conectaron previamente a SCCM o SCVMM.

Visualización o actualización de las consolas inscritas

Puede ver todas las consolas inscritas de Microsoft en OMIMSSC. Para ello, realice los siguientes pasos:

1. En el portal de administración de OMIMSSC, haga clic en **Configuración** y, a continuación, en **Registro de consolas**. Se muestran todas las consolas registradas.
2. Para ver la lista más reciente de consolas registradas, haga clic en **Actualizar**.

Cambio de la contraseña del dispositivo OMIMSSC

Para cambiar la contraseña de la VM del dispositivo OMIMSSC, realice los siguientes pasos:

1. Inicie la VM del dispositivo OMIMSSC e inicie sesión con las credenciales antiguas.
2. Navegue hasta **Cambiar la contraseña del administrador** y presione **Intro**. Se mostrará la pantalla para cambiar la contraseña.
3. Ingrese su contraseña actual y, a continuación, proporcione una contraseña nueva que coincida con los criterios indicados. Vuelva a introducir la contraseña nueva y presione **Intro**. Se mostrará el estado después de cambiar la contraseña.
4. Para volver a la página de inicio, presione **Intro**.

 **NOTA:** El dispositivo se reiniciará después de cambiar la contraseña.

Reparación o modificación de los instaladores

Para reparar cualquiera de los archivos del instalador, consulte los siguientes temas:

- [Reparación de la extensión de la consola de OMIMSSC para SCCM](#)
- [Reparación de la extensión de la consola de OMIMSSC para SCVMM](#)

Reparación de la extensión de la consola de OMIMSSC para SCCM

Para reparar los archivos de OMIMSSC en caso de que estén dañados, realice los siguientes pasos:

1. Ejecute la extensión de consola de OMIMSSC para el instalador de SCCM.
Se muestra la pantalla de **bienvenida**.
2. Haga clic en **Siguiente**.
3. En **Mantenimiento de programas**, seleccione **Reparar** y haga clic en **Siguiente**.
Aparecerá la pantalla **Listo para reparar el programa**.
4. Haga clic en **Instalar**.
Una pantalla de progreso muestra el progreso de la instalación. Una vez finalizada la instalación, aparece la ventana **Asistente de InstallShield completado**.
5. Haga clic en **Finalizar**.

Reparación de la extensión de la consola de OMIMSSC para SCVMM

Para reparar los archivos de OMIMSSC en caso de que estén dañados, realice los siguientes pasos:

1. Ejecute la extensión de consola de **OMIMSSC para el instalador de SCVMM**.
2. En **Mantenimiento de programas**, seleccione **Reparar** y haga clic en **Siguiente**.
3. En **Listo para reparar o quitar el programa**, haga clic en **Reparar**.
4. Cuando finalice la tarea de reparación, haga clic en **Finalizar**.

Modificación de las cuentas de SCCM y SCVMM en el portal de administración del dispositivo OMIMSSC

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

Puede modificar las contraseñas del administrador de SCCM y SCVMM desde el portal de administración de OMIMSSC. Este proceso es una actividad secuencial.

1. Modifique la contraseña de la cuenta de administrador de SCCM o SCVMM en Active Directory.
2. Modifique la contraseña en OMIMSSC.

Realice los siguientes pasos para cambiar la cuenta de administrador de SCCM o SCVMM en OMIMSSC:

1. En el portal de administración de OMIMSSC, haga clic en **Configuración** y, a continuación, en **Inscripción de consolas**.
Se muestran las consolas registradas.
2. Seleccione una consola por editar y haga clic en **Editar**.
3. Proporcione una nueva contraseña y, para guardar los cambios, haga clic en **Terminar**.

Después de actualizar la contraseña, vuelva a iniciar la consola de Microsoft y las extensiones de la consola de OMIMSSC con las nuevas credenciales.

Respaldo y restauración del dispositivo OMIMSSC

Use la opción **Respaldo de datos del dispositivo** del dispositivo OMIMSSC y guarde la información de OMIMSSC, como consolas inscritas de Microsoft, dispositivos detectados, perfiles, fuentes de actualización, plantillas operativas, licencias y trabajos terminados en las extensiones de la consola de OMIMSSC.

Temas:

- [Respaldo del dispositivo OMIMSSC](#)
- [Restaurar dispositivo OMIMSSC](#)

Respaldo del dispositivo OMIMSSC

Esta funcionalidad permite que se realice un respaldo de la base de datos del dispositivo OMIMSSC y de las configuraciones importantes. El archivo de respaldo se almacenará en la ruta del recurso compartido CIFS con una contraseña cifrada proporcionada por el usuario. Se recomienda que se realicen respaldos periódicos de los datos del dispositivo.

Requisitos previos:

- Asegúrese de crear el recurso compartido CIFS con las credenciales de acceso y permitir permisos de lectura y escritura.
- Asegúrese de que se utilice la misma contraseña de cifrado para el respaldo y la restauración. No se puede recuperar la contraseña de cifrado

Realice los siguientes pasos para respaldar los datos del dispositivo OMIMSSC en un recurso compartido CIFS.

 **NOTA:** Esta función está disponible a partir de la versión 7.2.1 de OMIMSSC y no está disponible en la consola negra.

1. Desde el portal de administración de OMIMSSC, haga clic en **Configuración** y, a continuación, en **Respaldo de dispositivo**.
2. En la página **Configuración y detalles del respaldo**, proporcione la ruta del recurso compartido CIFS para el respaldo en el formato `\\<IP address or FQDN>\<folder name>`.
3. Seleccione el **Perfil de credencial del recurso compartido CIFS** en el menú desplegable.
4. Introduzca la contraseña de cifrado en los campos **Contraseña** y **Vuelva a escribir la contraseña**.
5. Haga clic en **Probar conexión** para verificar la conectividad entre el dispositivo OMIMSSC y el recurso compartido CIFS. Asegúrese de que la carpeta de respaldo mencionada exista y sea accesible
6. Haga clic en **Respaldo** para respaldar los datos del dispositivo OMIMSSC.

Próximos pasos

Para volver a confirmar si el respaldo se realizó correctamente, acceda a la carpeta de respaldo. Se crearán dos archivos en la carpeta de respaldo en el siguiente formato:

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

 **NOTA:** La fecha y la hora que se muestran en los archivos de respaldo indicarán cuándo se realizó el respaldo. No cambie el nombre del archivo de respaldo.

Restaurar dispositivo OMIMSSC

Instale la extensión de la consola de la versión 7.2.1 de OMIMSSC antes de restaurar el dispositivo. Consulte la sección [Inicio del portal de administración de OMIMSSC para descargar los componentes de OMIMSSC](#).

Restaurar los datos del dispositivo OMIMSSC en cualquiera de los siguientes escenarios:

- Antes de actualizar a una versión nueva de OMIMSSC
- Antes de migrar de un dispositivo OMIMSSC a otro dispositivo OMIMSSC.

Restauración del dispositivo OMIMSSC

Requisitos previos:

Asegúrese de restaurar los datos antes de realizar cualquier operación en el nuevo dispositivo OMIMSSC.

Realice los siguientes pasos para restaurar los datos antiguos del dispositivo OMIMSSC en un nuevo dispositivo OMIMSSC.

1. Desde el portal de administración de OMIMSSC, haga clic en **Configuración** y, a continuación, en **Restaurar dispositivo**.

2. Hay dos opciones disponibles para restaurar los datos del dispositivo.

- Option 1: Restore using IP address

Esta opción se debe usar para restaurar los datos de las versiones 7.1, 7.1.1 y 7.2 de OMIMSSC.

En Dirección IP, proporcione la dirección IP del dispositivo OMIMSSC antiguo y haga clic en Restaurar.

NOTA: Los datos se restauran al nuevo dispositivo OMIMSSC.

- Opción 2: restaurar mediante un recurso compartido CIFS personalizado

Esta opción debe utilizarse para restaurar datos desde la versión 7.2.1 en adelante

NOTA: Las credenciales de acceso al recurso compartido CIFS se almacenan en la base de datos como perfil de credencial. Para mayores medidas de seguridad, se debe proporcionar la contraseña de cifrado para descifrar el archivo respaldado.

- a. Proporcione la ruta de la ubicación del recurso compartido CIFS en el formato `\\<IP address or FQDN>\<folder name>\<filename>.tar.gz`.
- b. Seleccione el Perfil de credencial para el recurso compartido CIFS en el menú desplegable.
- c. Ingrese la contraseña de cifrado del archivo y haga clic en Restaurar.

La página **Restaurar** se cerrará automáticamente.

3. Para ver el estado de restauración después de que se reinicie el dispositivo OMIMSSC, realice los siguientes pasos:

Se recomienda que espere algunos minutos antes de iniciar sesión para que se inicien todos los servicios.

- a. Inicie sesión en el portal de administración de OMIMSSC.
- b. Expanda **Configuración** y, a continuación, haga clic en **Registros**.
- c. Descargue el archivo `dlciappliance_main.log` y busque el siguiente mensaje para realizar una restauración correctamente:

```
Successfully restored OMIMSSC Appliance
```

Realice lo siguiente después de restaurar el dispositivo OMIMSSC antiguo:

- Se recomienda volver a crear los trabajos programados después de restaurar el dispositivo OMIMSSC antiguo.
- Para los perfiles de hipervisor exportados desde una versión anterior de OMIMSSC, asegúrese de editar el perfil a fin de proporcionar la ruta de archivo ISO y el perfil de credencial de Windows.

Desinstalación de OMIMSSC

Para desinstalar OMIMSSC, realice lo siguiente:

1. Cancele la inscripción de la consola de OMIMSSC desde el portal de administración de OMIMSSC. Para obtener más información, consulte [Cancelación de la inscripción de la consola de OMIMSSC](#).
2. Desinstale la extensión de la consola de OMIMSSC de la consola de Microsoft registrada. Para obtener más información, consulte [Desinstalación de la extensión de la consola de OMIMSSC para SCCM](#) o [Desinstalación de la extensión de la consola de OMIMSSC para SCVMM](#).
3. Elimine la VM del dispositivo OMIMSSC. Para obtener más información, consulte [Eliminación de la VM del dispositivo OMIMSSC](#).
4. Quite las cuentas específicas del dispositivo. Para obtener más información, consulte [Otras tareas de desinstalación](#).

Temas:

- [Cancelación de la inscripción de la consola de Microsoft en OMIMSSC OMIMSSC](#)
- [Desinstalación de la extensión de consola de OMIMSSC para SCCM](#)
- [Desinstalación de la extensión de la consola de OMIMSSC para SCVMM](#)
- [Otros pasos de desinstalación](#)
- [Eliminación de la máquina virtual del dispositivo](#)

Cancelación de la inscripción de la consola de Microsoft en OMIMSSC OMIMSSC

En caso de que tenga inscritas varias consolas de Microsoft en un dispositivo OMIMSSC, puede cancelar la inscripción de una consola y seguir trabajando con OMIMSSC. Para completar la desinstalación, consulte la *OpenManage Integration for Microsoft System Center Installation Guide* (Guía de instalación de OpenManage Integration para Microsoft System Center).

Para cancelar la inscripción de la consola de Microsoft, realice las siguientes acciones:

1. En OMIMSSC, haga clic en **Inscripción de consolas**. Aparecerán todas las consolas inscritas en el dispositivo OMIMSSC.
2. Seleccione la consola y haga clic en **Cancelar inscripción** para eliminar el registro de la consola en el dispositivo.
3. Desinstale el plug-in de la consola.

NOTA:

- Después de cancelar la inscripción de una consola y de desinstalarla, se transfieren los servidores host asociados con esta a la lista de servidores sin asignar de OMIMSSC.
4. (Opcional) En el caso de no poder acceder a la consola, haga clic en **Sí** cuando se le solicite cancelar la inscripción de la consola de manera forzada.
 - Si hay una consola de OMIMSSC abierta durante la cancelación de la inscripción, asegúrese de cerrar la consola de Microsoft para completar este proceso.
 - Para usuarios de SCVMM:
 - Si cancela la inscripción de una consola de SCVMM de OMIMSSC forzosamente cuando no se puede acceder al servidor de SCVMM, elimine de forma manual el **Perfil de aplicación** en SCVMM.

Desinstalación de la extensión de consola de OMIMSSC para SCCM

Haga doble clic en `OMIMSSC_SCCM_Console_Extension.exe`, seleccione **Quitar** y siga las instrucciones en pantalla.

Desinstalación de la extensión de la consola de OMIMSSC para SCVMM

Para desinstalar la extensión de la consola de OMIMSSC para SCVMM, realice los siguientes pasos:

1. Quite la extensión de la consola en **Desinstalar un programa**.
2. Quite la extensión de la consola de SCVMM.

Quitar la extensión de la consola de OMIMSSC para SCVMM

1. En **Panel de control**, haga clic en **Programas** y, a continuación, en **Desinstalar un programa**.
2. Seleccione **Complemento de consola para SCVMM** y, a continuación, haga clic en **Desinstalar**.

Quitar la extensión de la consola de OMIMSSC en SCVMM

1. En la consola de SCVMM, haga clic en **Configuración**.
2. Haga clic con el botón secundario en **OMIMSSC** y seleccione **Quitar**.

Otros pasos de desinstalación

Para eliminar la extensión de la consola de OMIMSSC de SCVMM, elimine las siguientes cuentas y perfiles:

- Cuentas de ejecución específicas del dispositivo
- OMIMSSC Perfil de aplicación

Eliminación de cuentas de ejecución específicas del dispositivo

Para eliminar las cuentas de ejecución específicas del dispositivo desde la consola de SCVMM, realice los siguientes pasos:

1. En la consola de SCVMM, haga clic en **Configuración**.
2. Haga clic en **Cuentas de ejecución**.
3. Desde la lista de cuentas, elimine las cuentas específicas del dispositivo.

Las cuentas específicas del dispositivo tienen el prefijo De11_.

Eliminación de perfil de aplicación de OMIMSSC

1. En la consola de SCVMM, haga clic en **Biblioteca, Perfiles** y, a continuación, haga clic en **Perfiles de aplicaciones**. Se muestran todos los perfiles de aplicación que se utilizan en SCVMM.
2. Seleccione y elimine el **Perfil de registro de OMIMSSC**.

Eliminación de la máquina virtual del dispositivo

Para eliminar la máquina virtual del dispositivo, realice los siguientes pasos:

1. En **Windows Server**, en **Administrador de Hyper-V**, haga clic con el botón secundario en el archivo de la VM del dispositivo y, a continuación, haga clic en **Apagar**.
2. Haga clic con el botón secundario en el archivo de la VM del dispositivo y, a continuación, haga clic en **Eliminar**.

Actualización de OMIMSSC para SCVMM

Después de instalar y configurar OMIMSSC, si hay disponible una actualización de Service Pack, puede usar la función Actualización de Service Pack de OMIMSSC para instalar las actualizaciones más recientes.

NOTA: La actualización de Service Pack a partir de versiones anteriores de OMIMSSC a OMIMSSC v7.2 o v7.2.1 no se encuentra disponible.

Para actualizar una versión anterior de OMIMSSC, realice un respaldo de los datos de la versión actual y restáurelo en el dispositivo OMIMSSC versión 7.2 o 7.2.1.

Para obtener más información sobre el respaldo y la restauración del dispositivo OMIMSSC, consulte las secciones [Respaldo del dispositivo OMIMSSC](#) y [Restauración del dispositivo OMIMSSC](#).

Temas:

- [Acerca de las actualizaciones de Service Pack](#)
- [Actualización de la extensión de la consola de OMIMSSC para SCCM](#)
- [Actualización de la extensión de la consola de OMIMSSC para SCVMM](#)

Acerca de las actualizaciones de Service Pack

Una vez que se libere el OMIMSSC, se debe compartir cualquier reparación de defectos críticos o funciones agregadas disponibles a modo de actualización o extensión en el dispositivo OMIMSSC existente. Puede actualizar Service Pack y otros elementos para el sistema operativo de OMIMSSC y para el dispositivo OMIMSSC.

- Puede colocar los archivos de Service Pack directamente en cualquier servidor HTTP y utilice los archivos de Service Pack para obtener actualizaciones.
- Puede aplicar estos Service Pack en forma incremental; sin embargo, una vez aplicados no puede revertirlos.
- Los Service Pack son acumulativos; es decir que el Service Pack más reciente tiene todas las reparaciones de versiones anteriores.

Los dos tipos de Service Pack de OMIMSSC son los siguientes:

- Service Pack del dispositivo OMIMSSC.
- Service Pack de infraestructura.

Las actualizaciones de Service Packs se pueden aplicar con dos métodos:

- Mediante un paquete offline.
- Mediante ***linux.dell.com***.

Para aplicar las actualizaciones de Service Pack mediante el paquete sin conexión, realice los siguientes pasos:

1. Descargue el Service Pack en Internet. Para obtener más información, consulte [Descarga de OMIMSSC en Internet](#)
2. Compruebe la lista de requisitos previos para las actualizaciones de Service Pack. Para obtener más información, consulte las [Instrucciones para actualizar los Service Packs](#)
3. Copie las actualizaciones de Service Pack descargadas en el repositorio. Para obtener más información, consulte [Copia de las actualizaciones de Service Pack en el repositorio](#).
4. Proporcione la información de la dirección URL del repositorio en el portal de administración del dispositivo OMIMSSC. Para obtener más información, consulte [Proporción de información de la dirección URL del repositorio](#).
5. Instale las actualizaciones de Service Pack. Para obtener más información, consulte [Instalación de actualizaciones de Service Pack](#).

Para aplicar las actualizaciones de Service Pack mediante el paquete en línea, realice los siguientes pasos:

1. Proporcione la información de la dirección URL del repositorio en el portal de administración del dispositivo OMIMSSC. Para obtener más información, consulte [Proporción de información de la dirección URL del repositorio](#).

2. Instale las actualizaciones de Service Pack. Para obtener más información, consulte [Instalación de actualizaciones de Service Pack](#).

Requisitos previos de instalación

- Asegúrese de implementar OMIMSSC para SCCM y SCVMM versión 7.1 o versión 7.1.1 o 7.2 antes de actualizar a OMIMSSC para SCCM y SCVMM versión 7.2.1.
- Asegúrese de que no se estén ejecutando trabajos. Si se están ejecutando trabajos, espere hasta que estos finalicen.
- Respalde los datos del dispositivo OMIMSSC.

 **NOTA:** Para obtener información sobre el procedimiento de respaldo, consulte la sección **Respaldo de dispositivo OMIMSSC**.

Instrucciones para actualizar los Service Pack

Para actualizar una versión anterior de OMIMSSC, realice un respaldo de los datos de la versión actual y, a continuación, actualice mediante Service Pack.

1. En el portal de administración de OMIMSSC, haga clic en **Configuración > Actualizaciones de Service Pack**
2. En el cuadro **URL del repositorio** ingrese la URL de la ubicación del repositorio de Service Pack utilizando uno de los siguientes métodos de actualización:
 - a. Para actualizar mediante el paquete sin conexión, en el cuadro **URL del Repositorio**, ingrese la información de la URL de la ubicación donde se guarda el Service Pack en el formato `http://<hostname o dirección IP> /OMIMSSC_v7.2_SP/RPM_Repository`.
 - b. Para actualizar mediante el sitio web de linux.dell.com, en el cuadro **dirección URL**, ingrese la información de la URL en el formato `http://linux.dell.com/repo/omimssc-sccm-scvmm/<versión de Service Pack>` y, en caso de ser necesario, proporcione detalles del servidor proxy y las credenciales para acceder al servidor y, a continuación, haga clic en **Guardar**.
3. Seleccione la casilla de verificación **Buscar actualizaciones**. La versión actual de OMIMSSC y Service Pack se muestran en la pantalla.
4. Haga clic en **Aplicar** y luego en **Aceptar**
5. Diríjase a **Configuración > Registros >** en el directorio de registros de actualización para ver o descargar los archivos de registro para la actualización de Service Pack, seleccione el directorio <número de versión de Service Pack>, por ejemplo, el directorio <folder name> para ver o descargar los archivos de registro para la actualización de Service Pack.
6. Inicie sesión en el **Portal de Administración** y, a continuación, elimine el historial del caché del navegador.
7. Una vez finalizada la actualización del Service Pack, reinicie el dispositivo de forma manual.

Para obtener más información sobre cómo crear repositorios de actualización de Service Pack, consulte la sección [Acerca de las actualizaciones de Service Pack](#).

Copia de las actualizaciones de Service Pack en el repositorio

- Guarde el Service Pack descargado en un repositorio.
- Asegúrese de que los formatos de todos los archivos en el paquete del servidor sean compatibles con el servidor HTTP. Si no es así, comuníquese con el administrador de HTTP para agregar la compatibilidad. Se admiten los siguientes formatos de archivo:
 - .RPM
 - .XML
 - .TXT
 - .BZ2

Realice lo siguiente para habilitar el formato de archivo .BZ2:

1. Abra el Administrador de IIS en el servidor donde se guardan los archivos repo.
2. Expanda el nombre del host. Haga clic en **Sitios** y, a continuación, en **Sitio web predeterminado**.
3. En el panel **Acción** haga clic en **Agregar**.
Se muestra la ventana **Add MIME Type Agregar tipo MIME**.
4. Proporcione la **Extensión de nombre de archivo** como **.BZ2** y el **tipo MIME** como **APP/BZ2**, y haga clic en **Aceptar**.

Preparación del repositorio

1. Coloque los archivos de Service Pack directamente en el servidor HTTP.
2. Haga doble clic en el Service Pack descargado y descomprima los archivos en una ubicación.
3. Copie los archivos descomprimidos en el sitio HTTP.

Proporcione información de las direcciones URL del repositorio para las actualizaciones de Service Pack

Para actualizar OMIMSSC, proporcione la información de la dirección URL en la que se encuentran las actualizaciones de Service Pack.

Para actualizar OMIMSSC con las actualizaciones de Service Pack, realice los siguientes pasos:

1. En **OMIMSSC**, seleccione **Configuración Actualizaciones de Service Pack**.
2. Para actualizar mediante el paquete sin conexión, ingrese la información de URL en el formato `http://<servername>:<portname>/<repository path>` en la **URL del Repositorio** y, si es necesario, proporcione los detalles del servidor proxy y las credenciales para acceder al servidor. A continuación, haga clic en **Guardar**.

 **NOTA:** Asegúrese de que el nombre del host especificado en la URL no contenga un guion bajo (_).

Para actualizar mediante el sitio web linux.dell.com, in **URL del repositorio**, proporcione la información de URL en el siguiente formato `http://linux.dell.com/repo/omimssc-sccm-scvmm/<versión de Service Pack>` y, si es necesario, proporcione los detalles del servidor proxy y las credenciales para acceder al servidor. A continuación, haga clic en **Guardar**.

Instalación de actualizaciones de Service Pack

Verifique si la información del URL del repositorio está disponible y se incluye en la página **Actualizaciones de Service Pack**. Para obtener más información, consulte [Cómo proporcionar la información del URL del repositorio](#).

Para instalar actualizaciones de Service Pack:

1. Después de colocar el Service Pack en el sitio HTTP, en **Portal de administración de OMIMSSC > Configuración > Actualizaciones de Service Pack**, haga clic en **Buscar actualizaciones**.

Para OMIMSSC, se muestra la versión existente y la versión disponible de Service Pack en el repositorio.

Si es necesario, puede ver las Notas de la versión.

2. Haga clic en **Aplicar** y después en **Aceptar**.
3. Una vez finalizada la actualización, inicie sesión en el portal de administración de OMIMSSC y, a continuación, borre el historial de la memoria caché del navegador.

Después de la instalación:

Para verificar la actualización de Service Pack:

1. En el Portal de administración de OMIMSSC, en **Acerca de**, vea los detalles de la versión de la actualización de Service Pack.
2. Para obtener más información, en Portal de administración de OMIMSSC, seleccione **Configuración > Registros**.
3. En el directorio **upgradelogs**, para ver o descargar los archivos de registro para la actualización de Service Pack, seleccione el directorio **<número de versión de service pack>** (por ejemplo, el directorio 1.2.0.207) para ver o descargar los archivos de registro para la actualización de Service Pack.
4. Si la actualización de Service Pack falla, visite dell.com/support.
5. Reinicie el dispositivo de forma manual.

 **NOTA:** Una vez finalizada la actualización de Service Pack,

- Actualice la extensión de la consola de OMIMSSC para SCCM.
- Actualice la extensión de la consola de OMIMSSC para SCVMM.

Actualización de la extensión de la consola de OMIMSSC para SCCM

Asegúrese de respaldar el antiguo dispositivo OMIMSSC. Para obtener más información, consulte [Respaldo del dispositivo OMIMSSC](#).

1. Desde el portal de administración de OMIMSSC, haga clic en **Descargar instalador** y guarde el instalador en una ubicación.
2. Ejecute el instalador de OMIMSSC.
3. En el mensaje que le preguntará si desea actualizar, haga clic en **Sí**.
4. En la página de bienvenida de OMIMSSC, haga clic en **Siguiente**.
5. En la pantalla **Acuerdo de licencia**, seleccione **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
6. En la página **Preparado para instalar el programa**, haga clic en **Instalar**.
7. En la página **Asistente InstallShield completado**, haga clic en **Terminar** para completar la instalación.

Actualización de la extensión de la consola de OMIMSSC para SCVMM

Asegúrese de respaldar el antiguo dispositivo OMIMSSC. Para obtener más información, consulte [Respaldo del dispositivo OMIMSSC](#).

1. Desde el portal de administración de OMIMSSC, haga clic en **Descargar instalador** y guarde el instalador en una ubicación.
2. Ejecute el instalador de OMIMSSC.
3. En el mensaje que le preguntará si desea actualizar, haga clic en **Sí**.
4. En la página de bienvenida de OMIMSSC, haga clic en **Siguiente**.
5. En la pantalla **Acuerdo de licencia**, seleccione **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
6. En la página **Preparado para instalar el programa**, haga clic en **Instalar**.
7. En la página **Asistente InstallShield completado**, haga clic en **Terminar** para completar la instalación.
8. Elimine la extensión de la consola de OMIMSSC para SCVMM y vuelva a importarla. Para obtener información sobre la eliminación de la consola, consulte [Eliminación de la extensión de la consola de OMIMSSC para SCVMM](#).

Reinicio del dispositivo OMIMSSC

Realice los siguientes pasos para reiniciar el dispositivo OMIMSSC:

1. Inicie la VM del dispositivo OMIMSSC e inicie sesión en ella.
2. Navegue hasta **Reiniciar este dispositivo virtual** y presione **Intro**.
3. Para confirmar, haga clic en **Sí**.
El dispositivo OMIMSSC se reinicia junto con todos los servicios obligatorios.
4. Inicie sesión en el dispositivo OMIMSSC después de que la VM se reinicie.

Cierre de sesión del dispositivo OMIMSSC

1. Inicie la VM del dispositivo OMIMSSC e inicie sesión en ella.
2. Vaya a **Cerrar sesión** y presione **Intro**.

Administración de perfiles

Los perfiles contienen todos los datos necesarios para realizar cualquier operación en OMIMSSC.

Temas:

- [Acerca del perfil de credenciales](#)
- [Acerca del perfil de hipervisor \(para usuarios de SCVMM\)](#)

Acerca del perfil de credenciales

Los perfiles de credencial facilitan el uso y la administración de las credenciales de usuario mediante la autenticación de las capacidades del usuario basadas en funciones. Cada perfil de credencial contiene un nombre de usuario y una contraseña para una única cuenta de usuario.

OMIMSSC utiliza perfiles de credencial para conectarse al iDRAC de los sistemas administrados. Además, puede utilizar perfiles de credencial para acceder al sitio FTP y a los recursos disponibles en los recursos compartidos de Windows, y para trabajar con diferentes funciones del iDRAC.

Puede crear cuatro tipos de perfiles de credenciales:

- Perfil de credencial de dispositivo: se utiliza para iniciar sesión en iDRAC o CMC. Además, puede utilizar este perfil para descubrir un servidor, resolver problemas de sincronización e implementar un sistema operativo. Este perfil es específico de una consola. Puede utilizar y administrar este perfil solo en la consola en la cual se crea.
- Perfil de credencial de Windows: se utiliza para acceder a carpetas de recursos compartidos en el sistema operativo Windows
- Perfil de credencial de FTP: se utiliza para acceder al sitio FTP
- Credenciales del servidor proxy: se utilizan para proporcionar credenciales de proxy para acceder a los sitios FTP y obtener actualizaciones.

NOTA: Todos los perfiles son recursos compartidos, con la excepción del perfil de dispositivo. Puede utilizar y administrar estos perfiles desde cualquier consola inscrita.

Perfil de credencial predefinida

Una cuenta de **FTP PREDETERMINADO DE SISTEMA** es un perfil de credencial disponible en OMIMSSC. El perfil de credencial predefinido es de tipo FTP y su **nombre de usuario** y **contraseña** son **anónimo**. Utilice este perfil para acceder a `ftp.dell.com`

Creación de perfil de credenciales

Tenga en cuenta los siguientes puntos cuando cree un perfil de credencial:

- Durante el descubrimiento automático, si un perfil de credencial predeterminado no está disponible para iDRAC, entonces se utilizan las credenciales predeterminadas de iDRAC. El nombre de usuario iDRAC predeterminado es `root` y la contraseña es `calvin`.
- Para obtener información acerca de los sistemas modulares, se accede al servidor modular con el perfil de CMC predeterminado. El nombre de usuario del perfil CMC predeterminado es `root` y la contraseña es `calvin`.
- (Solo para usuarios de SCVMM) Cuando se crea un perfil de credenciales de tipo de dispositivo, se crea una **Cuenta de ejecución** asociada en **SCVMM** para administrar el dispositivo y el nombre de la **cuenta de ejecución** es `Dell_CredentialProfileName`.
- Asegúrese de no editar o eliminar la **cuenta de ejecución** en SCVMM.

1. En OMIMSSC, realice cualquiera de los siguientes pasos para crear un **Perfil de credencial**:

- En el panel de OMIMSSC, haga clic en **Crear perfil de credencial**.
- En el panel de navegación, haga clic en **Perfiles > Perfil de credencial** y, luego, en **Crear**.

2. En **Tipo de credencial**, seleccione el tipo de perfil de credencial que desea utilizar.
3. Escriba un nombre y una descripción del perfil.

NOTA: La opción **Perfil predeterminado para** se aplica solamente a un perfil de credencial de tipo Dispositivo.

4. En **Credenciales**, escriba el nombre de usuario y la contraseña.
 - Si va a crear un **perfil de credencial de dispositivo**, seleccione la opción **Perfil predeterminado para**, a fin de hacer que este perfil sea el perfil predeterminado para iniciar sesión en iDRAC o CMC. Seleccione **Ninguno** si opta por no establecer el perfil como un perfil predeterminado.
 - Si va a crear un **perfil de credencial de Windows**, proporcione los detalles del dominio en **Dominio**.

NOTA: Al crear el perfil de credencial para la inscripción de la consola, si el nombre de NETBIOS está configurado en Active Directory (AD), proporcione el nombre de NETBIOS como dominio. Si no se ha configurado el nombre de NETBIOS en AD, proporcione el nombre de dominio con los detalles de dominio de nivel superior (TLD).

Por ejemplo, si el nombre de dominio es `mydomain` y el TLD es `com`, escriba el nombre de dominio en el perfil de credencial como: `mydomain.com.mydomain.com`

- Si va a crear **credenciales de servidor proxy**, proporcione la URL del servidor proxy con el formato `http://hostname:port` o `http://IPaddress:port` en **URL de servidor proxy**.

5. Para crear el perfil, haga clic en **Completar**.

NOTA: Cuando crea un perfil de credenciales de tipo de dispositivo en SCVMM, crea una **RunAsAccount** correspondiente con un nombre con el prefijo **Dell_**. Asegúrese de que el usuario inscrito tenga acceso a la **RunAsAccount** correspondiente para operaciones como la implementación de sistema operativo, la cual consume el perfil de credenciales del dispositivo creado.

Modificación de perfil de credenciales

Tenga en cuenta lo siguiente antes de modificar un perfil de credencial:

- Después de crear el tipo de un perfil de credencial, no podrá modificarlo. Sin embargo, puede modificar otros campos.
- No puede modificar un perfil de credencial si está en uso.

NOTA: Los pasos para modificar cualquier tipo de perfil de credencial son los mismos.

1. Seleccione el perfil de credencial que desea modificar, haga clic en **Editar** y actualice el perfil.
2. Para guardar los cambios realizados, haga clic en **Guardar**.

Para ver los cambios realizados, actualice la página **Perfil de credencial**.

Eliminación de un perfil de credenciales

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 la **cuenta de ejecución** en SCVMM, el perfil de credencial correspondiente no está disponible en OMIMSSC.
- Para eliminar el perfil de credencial utilizado para descubrir servidores, elimine el servidor descubierto y, luego, elimine el perfil de credencial.
- Para eliminar un perfil de credenciales de tipo de dispositivo que se utiliza para la implementación, primero elimine los servidores implementados en el entorno SCVMM y, luego, elimine el perfil de credencial.
- No puede eliminar un perfil de credenciales que se utilice en un origen de actualizaciones.

NOTA: Los pasos para eliminar cualquier tipo de perfil de credencial son los mismos.

Seleccione el perfil de credencial que desea eliminar y, luego, haga clic en **Eliminar**.

Para ver los cambios realizados, actualice la página **Perfil de credencial**.

Acerca del perfil de hipervisor (para usuarios de SCVMM)

Un perfil de hipervisor contiene una ISO de WinPE personalizada (se utiliza para implementar el hipervisor), un grupo de hosts y un perfil de host extraídos de SCVMM, además de controladores LC para su inyección. Solo los usuarios de la extensión de consola de OMIMSSC para SCVMM pueden crear y administrar perfiles de hipervisor.

Creación de perfil de hipervisor

Cree un perfil de hipervisor y utilícelo para implementar hipervisores.

- Actualice la imagen ISO de WinPE y acceda a la carpeta compartida en la que se guarda la imagen. Para obtener más información acerca de cómo actualizar la imagen de WinPE, consulte [Actualización de WinPE](#).
 - En SCVMM, cree un grupo de hosts, un perfil de host o un perfil de equipo físico. Para obtener información acerca de cómo crear grupos de hosts en SCVMM, consulte la documentación de Microsoft.
1. En OMIMSSC, realice una de las siguientes tareas:
 - En el tablero de OMIMSSC, haga clic en **Crear perfil de hipervisor**.
 - En el panel de navegación izquierdo, haga clic en **Perfiles y plantillas, Perfil de hipervisor** y, luego, en **Crear**.

Se muestra la opción **Asistente de perfil de hipervisor**.

2. En la página **Bienvenido**, haga clic en **Siguiente**.
3. En **Perfil de hipervisor**, ingrese un nombre y una descripción para el perfil; luego, haga clic en **Siguiente**.
4. En la página **Información de SCVMM**,
 - a. Para **Destino de grupo de hosts de SCVMM**, seleccione un grupo de hosts de SCVMM en el menú desplegable para agregar el host a este grupo.
 - b. Desde **Perfil de host/perfil de equipo físico de SCVMM**, seleccione un perfil de host o un perfil de equipo físico desde SCVMM que incluya la información de configuración que se va a aplicar en los servidores.

En SCVMM, seleccione uno de los siguientes métodos de partición de disco en un **perfil de equipo físico**:

 - Cuando arranque el sistema desde el modo UEFI, seleccione la opción **Tabla de partición de GUID (GPT)**.
 - Cuando arranque el sistema desde el modo BIOS, seleccione la opción **Registro de placa maestra (MBR)**.
5. En **Fuente de imagen de arranque de WinPE**, ingrese los siguientes detalles y haga clic en **Siguiente**.
 - a. Para **Nombre de ISO de WinPE en red**, proporcione la ruta a la carpeta del recurso compartido que tenga el nombre de archivo WinPE actualizado. Para actualizar el archivo WinPE, consulte [Actualización de WinPE](#).
 - b. Para **Perfil de credenciales**, seleccione las credenciales que cuentan con acceso a la carpeta del recurso compartido que tiene el archivo WinPE.
 - c. (Opcional) Para crear un perfil de credencial de Windows, haga clic en **Crear nuevo**. Para obtener información acerca de cómo crear un perfil de credencial, consulte [Crear perfil de credencial](#).
6. (Opcional) Para activar la inyección de controlador de LC, realice los pasos siguientes:

 **NOTA:** Asegúrese de seleccionar la casilla de verificación **Activar inyección de controladores de Dell Lifecycle Controller**, puesto que los paquetes más recientes de controladores del sistema operativo para tarjetas NIC están disponibles en los controladores de sistema operativo más recientes.

 - a. Seleccione el sistema operativo que desea implementar, de modo que se seleccionen los controladores correspondientes.
 - b. Seleccione **Activar inyección de controladores de LC**.
 - c. Seleccione la versión del hipervisor en **Versión de hipervisor**.
7. En **Resumen**, haga clic en **Terminar**.

Para ver los cambios realizados, actualice la página **Perfil de hipervisor**.

Modificación de un perfil de hipervisor

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 modificar el nombre de ISO de WinPE. Sin embargo, no puede modificar la imagen ISO.

1. Seleccione el perfil que desea modificar y haga clic en **Editar**.
2. Ingrese los detalles y haga clic en **Completar**.

Para ver los cambios realizados, actualice la página **Perfil de hipervisor**.

Eliminación de perfil de hipervisor

Seleccione el perfil de hipervisor que desea eliminar y haga clic en **Eliminar**.

Para ver los cambios realizados, actualice la página **Perfil de hipervisor**.

Descubrimiento de dispositivos y sincronización de servidores con la consola de MSSC

El descubrimiento es el proceso de agregar sistemas modulares compatibles y servidores PowerEdge de bajo nivel, servidores host o nodos a OMIMSSC.

La sincronización con la consola MSSC es el proceso de agregar servidores host desde una consola Microsoft registrada (SCCM o SCVMM) a OMIMSSC. Por lo tanto, si utiliza alguno de los procesos, puede agregar dispositivos a OMIMSSC. Solo puede administrar dispositivos en OMIMSSC después de descubrirlos.

Temas:

- [Descubrir dispositivos en OMIMSSC](#)
- [Sincronización de extensión de consola de OMIMSSC con SCCM inscrito](#)
- [Resolver errores de sincronización](#)
- [Ver el modo de bloqueo del sistema](#)
- [Eliminar servidores en OMIMSSC](#)

Descubrir dispositivos en OMIMSSC

Descubra sistemas modulares, hosts y servidores sin asignar MX7000 en OMIMSSC. La información acerca de los dispositivos descubiertos se guarda en el dispositivo de OMIMSSC.

Puede descubrir servidores Dell EMC mediante sus direcciones IP de iDRAC utilizando los siguientes métodos:

- [Descubrimiento de servidores mediante descubrimiento automático](#)
- [Descubrimiento de servidores mediante descubrimiento manual](#)

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

Descubra sistemas modulares con la dirección IP del dispositivo utilizando el método descrito en [Descubrir sistemas modulares mediante el descubrimiento manual](#).

Descubrimiento de dispositivos en la extensión de consola de OMIMSSC para SCCM

Descubra dispositivos en la extensión de consola de OMIMSSC para SCCM. Luego de descubrir un servidor, este se agrega a un grupo predefinido en OMIMSSC y a uno de los siguientes grupos o recopilaciones predefinidas de SCCM (**recopilación Todos los servidores Dell Lifecycle Controller** y **recopilación Importar servidor Dell**) que se crean en las **Recopilaciones de dispositivos**.

Si el servidor descubierto no está presente en SCCM, o si no hay grupos o recopilaciones predefinidas en SCCM, se crean las recopilaciones predefinidas y se agrega el servidor descubierto al grupo correspondiente.

Descubrimiento de dispositivos en la extensión de consola de OMIMSSC SCVMM

Descubra sistemas modulares, hosts Hyper-V y servidores sin asignar en la extensión de consola de OMIMSSC para SCVMM. Después del descubrimiento, los dispositivos se agregan a los respectivos grupos de actualización predefinidos.

Requisitos del sistema para los sistemas administrados

Los sistemas administrados son dispositivos administrados mediante OMIMSSC. A continuación, se muestran los requisitos de sistema para detectar servidores mediante las extensiones de la consola de OMIMSSC:

- OMIMSSC La extensión de la consola de OMIMSSC para SCCM admite modelos de servidor modular, monolítico y en torre en servidores desde la 12.ª generación en adelante.
- OMIMSSC La extensión de la consola de OMIMSSC para SCVMM admite modelos de servidor modular y monolítico en servidores desde la 12.ª generación en adelante.
- Para la configuración de origen y de destino, utilice el mismo tipo de discos: solo unidad de estado sólido (SSD), SAS o solo unidades Serial ATA (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 opción Recopilar inventario del sistema durante el reinicio (CSIOR) en sistemas administrados. Para obtener más información, consulte la documentación de iDRAC.

Descubrimiento de servidores mediante descubrimiento automático

Para descubrir servidores automáticamente, conecte los servidores a la red y enciéndalos. OMIMSSC descubre automáticamente los servidores sin asignar mediante la función de activación remota del iDRAC. OMIMSSC opera como el servidor de aprovisionamiento y utiliza la referencia del iDRAC para descubrir servidores automáticamente.

1. En OMIMSSC, cree un perfil de credencial de tipo de dispositivo ingresando las credenciales de iDRAC y convirtiéndolas en el valor predeterminado para los servidores. Para obtener información acerca de cómo crear un perfil de credencial, consulte [Crear perfil de credencial](#).
2. Desactive la cuenta de administrador existente en la configuración de iDRAC en el dispositivo administrado.
 **NOTA:** Se recomienda tener una cuenta de usuario invitado con privilegios de operador para iniciar sesión en iDRAC en el caso de que falle el descubrimiento automático.
3. Habilite la función de descubrimiento automático en la configuración de iDRAC del dispositivo administrado. Para obtener más información, consulte la documentación de iDRAC.
4. En la configuración de iDRAC del dispositivo administrado, ingrese la IP del dispositivo de OMIMSSC en **IP del servidor de aprovisionamiento** y, luego, reinicie el servidor.

Descubrir servidores mediante el descubrimiento manual

Descubra servidores PowerEdge manualmente mediante una dirección IP o un rango IP. Para descubrir servidores, ingrese la dirección IP de iDRAC y las credenciales del tipo de dispositivo de un servidor. Cuando descubra servidores mediante un rango de IP, incluya el rango de inicio y fin, y las credenciales del tipo de dispositivo de un servidor para especificar un rango de IP (IPv4) dentro de una subred.

Asegúrese de que haya un perfil de credencial predeterminado disponible.

1. En la consola de OMIMSSC, realice uno de los pasos siguientes:
 - En el tablero, haga clic en **Descubrir servidores**.
 - En el panel de navegación, haga clic en **Configuración e implementación**, en **Vista de servidor** y, luego, en **Descubrir**.
2. En la página **Descubrir**, seleccione la opción requerida:
 - **Descubrir mediante una dirección IP:** para descubrir un servidor utilizando una dirección IP.

- **Descubrir mediante un rango IP:** para descubrir todos los servidores dentro de un rango de IP.
3. Seleccione el perfil de credencial del tipo de dispositivo, o bien haga clic en **Crear nuevo** para crear un perfil de credenciales del tipo de dispositivo.
El perfil seleccionado se aplica a todos los servidores.
 4. En **Dirección IP de iDRAC**, ingrese la dirección IP del servidor que desea descubrir.
 5. En **Detectar mediante una dirección IP o un rango de direcciones IP**, realice alguna de las acciones siguientes:
 - En **Rango de inicio de dirección IP** y **Rango de fin de dirección IP**, ingrese el rango de dirección IP que desea incluir, el cual es el rango de inicio y fin.
 - Seleccione **Habilitar rango de exclusión** si desea excluir un rango de dirección IP. En **Rango de inicio de la dirección IP** y **Rango de fin de la dirección IP**, ingrese el rango que desea excluir.
 6. Ingrese un nombre único de trabajo y una descripción para el trabajo; luego, haga clic en **Completar**.
Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Se muestra la página **Centro de trabajos y registros**. Amplíe el trabajo de detección para ver el progreso del trabajo en la pestaña **En ejecución**.

Luego de descubrir un servidor, este se agrega a la pestaña **Hosts** o **Sin asignar** en la página **Vista de servidor** de la sección **Configuración e implementación**.

- Cuando descubra un servidor con un sistema operativo ya implementado y si el servidor ya está presente en la consola SCCM o SCVMM, entonces el servidor aparece como un servidor host en la pestaña **Host**.
- Cuando descubre un servidor PowerEdge que no aparece en SCCM o SCVMM, entonces el servidor aparece en la lista como un servidor sin asignar en la pestaña **Sin asignar** de todas las extensiones de consola de OMIMSSC; en el caso de varias consolas Microsoft, el servidor queda inscrito a un único dispositivo de OMIMSSC.

Luego de descubrir un servidor, el servidor se marca como hardware compatible cuando contiene versiones admitidas de firmware de LC, iDRAC y BIOS para trabajar con OMIMSSC. Para ver las versiones de firmware de los componentes del servidor, pase el cursor sobre la columna **Compatibilidad del hardware** junto a la fila del servidor. Para obtener información acerca de las versiones compatibles, consulte las *Notas de la versión de OpenManage Integration para Microsoft System Center*.

Se consume una licencia por cada servidor descubierto. El conteo de **nodos de licencia** en la página **Centro de licencias** disminuye junto con la cantidad de servidores descubiertos.

NOTA: Para trabajar con los servidores descubiertos en versiones anteriores del dispositivo de OMIMSSC, vuelva a descubrir los servidores.

NOTA: Cuando inicia sesión en OMIMSSC como un administrador delegado, puede ver todos los servidores host y los servidores sin asignar que no son específicos del usuario que inició sesión. Por lo tanto, no puede realizar ninguna operación en esos servidores. Asegúrese de contar con los privilegios necesarios antes de realizar cualquier operación en esos servidores.

Descubrir MX7000 mediante el descubrimiento manual

Para detectar manualmente un sistema modular MX7000 PowerEdge mediante una dirección IP o un rango IP, ingrese la dirección IP de un sistema modular y las credenciales de tipo de dispositivo del sistema modular. Cuando descubra sistemas modulares mediante un rango de IP, incluya el rango de inicio y fin, y las credenciales del tipo de dispositivo de los sistemas modulares para especificar un rango de IP (IPv4) dentro de una subred.

Asegúrese de que el perfil de credencial predeterminado de un sistema modular que desea descubrir esté disponible.

Para descubrir sistemas modulares, realice los pasos siguientes:

1. En OMIMSSC, haga clic en **Configuración e implementación**, en **Vista de sistemas modulares** y, luego, en **Descubrir**.
2. En la página **Descubrir**, seleccione la opción requerida:
 - **Descubrir mediante una dirección IP:** para descubrir un sistema modular a través de una dirección IP.
 - **Descubrir mediante un rango IP:** para descubrir todos los sistemas modulares dentro de un rango de IP.
3. Seleccione el perfil de credencial del tipo de dispositivo, o bien haga clic en **Crear nuevo** para crear un perfil de credenciales del tipo de dispositivo.
El perfil seleccionado se aplica a todos los servidores.
4. En **Dirección IP**, ingrese la dirección IP del sistema modular que desee descubrir.
5. En **Descubrir mediante una dirección IP o un rango de direcciones IP**, realice alguna de las siguientes acciones:

- En **Rango de inicio de dirección IP** y **Rango de fin de dirección IP**, ingrese el rango de dirección IP que desea incluir, el cual es el rango de inicio y fin.
 - Seleccione **Habilitar rango de exclusión** si desea excluir un rango de dirección IP. En **Rango de inicio de la dirección IP** y **Rango de fin de la dirección IP**, ingrese el rango que desea excluir.
6. En **Métodos de descubrimiento de sistemas modulares**, seleccione una de las siguientes opciones:
- **Descubrimiento ligero**: descubre sistemas modulares y también la cantidad de servidores en el sistema modular.
 - **Descubrimiento exhaustivo**: descubre sistemas modulares y los dispositivos presentes en el sistema modular, como los módulos de entrada/salida (IOM) y los dispositivos de almacenamiento.
- NOTA:** Para realizar un descubrimiento exhaustivo de MX7000 y sus componentes, asegúrese de que PowerEdge MX7000 y todos sus componentes estén habilitados con dirección IPv4.
7. Ingrese un nombre de trabajo único y haga clic en **Completar**.
- Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.
- Para ver el progreso del trabajo en la pestaña **En ejecución**, expanda el trabajo de descubrimiento en el **Centro de trabajos y registros**.

Sincronización de extensión de consola de OMIMSSC con SCCM inscrito

Puede sincronizar todos los servidores (hosts y sin asignar) desde un SCCM inscrito con OMIMSSC. Además, obtendrá la información de inventario de firmware más reciente relacionada con los servidores después de la sincronización.

Antes de sincronizar OMIMSSC y la consola de SCCM inscrita, asegúrese de que se cumplan los siguientes requisitos:

- Tenga a mano detalles del perfil de credencial iDRAC predeterminado para los servidores.
- Actualice la **recopilación predeterminada de Dell** antes de sincronizar OMIMSSC con SCCM. Sin embargo, si se descubre un servidor sin asignar en SCCM, este se agrega a **Importar recopilación de servidores Dell**. Para agregar este servidor a la **recopilación predeterminada de Dell**, agregue la dirección IP de iDRAC del servidor en la página **OOB**.
- Asegúrese de que no hay entradas duplicadas de dispositivos en SCCM.

Después de sincronizar OMIMSSC con SCCM, si el dispositivo no está presente en SCCM, entonces se crea la recopilación **Todos los servidores Dell Lifecycle Controller** y la recopilación **Importar servidor Dell** en **Recopilaciones de dispositivos** y se agrega el servidor al grupo respectivo.

Sincronización de extensión de consola de OMIMSSC con SCVMM inscrito

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

Tenga en cuenta lo siguiente antes de sincronizar OMIMSSC con SCVMM:

- Tenga a mano detalles del perfil de credencial iDRAC predeterminado para los servidores.
- Si la controladora de administración de placa base (BMC) del servidor host no está configurada con la dirección IP de iDRAC, entonces no puede sincronizar el servidor host con OMIMSSC. Por lo tanto, configure BMC en SCVMM (para obtener más información, consulte el artículo de MSDN en technet.microsoft.com) y, luego, sincronice OMIMSSC con SCVMM.
- SCVMM admite varios hosts en el entorno y, por este motivo, la sincronización es una tarea de ejecución larga.

Sincronizar con consola Microsoft inscrita

Para agregar servidores administrados en la consola Microsoft a OMIMSSC, realice los siguientes pasos:

En OMIMSSC, haga clic en **Configuración e implementación**, haga clic en **Vista de servidor** y, luego, en **Sincronizar con OMIMSSC** para sincronizar todos los hosts que aparecen en la MSSC inscrita con el dispositivo OMIMSSC.

Resolver errores de sincronización

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

NOTA: Es posible que los servidores no estén sincronizados debido a problemas como credenciales no válidas, la dirección IP del iDRAC, conectividad o problemas de otro tipo; asegúrese de resolver primero los problemas y, luego, sincronice.

NOTA: Durante la resincronización, los servidores host que se eliminaron del entorno MSSC inscrito se mueven a la pestaña **Servidores sin asignar** en las extensiones de consola de OMIMSSC. Si un servidor quedó fuera de servicio, entonces elimine ese servidor de la lista de servidores sin asignar.

Para volver a sincronizar servidores con problemas de perfil de credencial:

1. En OMIMSSC, haga clic en **Configuración e implementación**, haga clic en **Vista de servidor** y, luego, en **Resolver errores de sincronización**.
2. Seleccione los servidores que se deben volver a sincronizar y seleccione el perfil de credencial o haga clic en **Crear nuevo** para crear un perfil de credencial.
3. Proporcione un nombre para la tarea y, de ser necesario, seleccione la opción **Ir a la lista de tareas** para ver el estado del trabajo automáticamente una vez que este se envíe.
4. Haga clic en **Completar** para enviar el trabajo.

Ver el modo de bloqueo del sistema

La configuración Modo de bloqueo del sistema está disponible en el iDRAC para los servidores de 14.^a generación en adelante. Cuando se activa la configuración, esta bloquea la configuración del sistema e incluye las actualizaciones de firmware. Tras activar el modo de bloqueo del sistema, los usuarios no pueden cambiar ningún valor de configuración. Esta configuración se diseñó para proteger el sistema de cambios no intencionales. Para llevar a cabo alguna operación en los servidores administrados, asegúrese de deshabilitar la configuración en su consola de iDRAC. En la consola OMIMSSC, el estado Modo de bloqueo del sistema se representa con una imagen de candado antes de la dirección IP de iDRAC del servidor.

- Aparece una imagen de candado junto a la IP de iDRAC de los servidores si la configuración está activada en ese sistema.
- Si la configuración está desactivada en ese sistema, aparece una imagen de candado abierto junto a la IP de iDRAC de los servidores.

NOTA: Antes de iniciar las extensiones de consola de OMIMSSC, verifique la configuración de iDRAC Modo de bloqueo del sistema en los servidores administrados.

Para obtener más información acerca del Modo de bloqueo del sistema de iDRAC, consulte la documentación de iDRAC disponible en dell.com/support.

Eliminar servidores en OMIMSSC

Para eliminar un servidor, realice los pasos siguientes:

Tenga en cuenta los siguientes puntos antes de eliminar un servidor:

- Después de eliminar un servidor, se abandona la licencia consumida.
 - Puede eliminar un servidor que aparece en OMIMSSC según los siguientes criterios:
 - Un servidor sin asignar que aparece en la pestaña **Servidores sin asignar**.
 - Si elimina un servidor host aprovisionado en el SCCM o SCVMM inscrito y que está presente en OMIMSSC en la pestaña **Hosts**, primero elimine el servidor en SCCM o SCVMM; Luego, elimine el servidor en OMIMSSC.
1. En la consola de OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de servidor**:
 - Para eliminar servidores sin asignar: en la pestaña **Servidores sin asignar**, seleccione el servidor y haga clic en **Eliminar**.
 - Para eliminar servidores host: en la pestaña **Servidores host**, seleccione el servidor y haga clic en **Eliminar**.
 2. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

Eliminar sistemas modulares en OMIMSSC

Para eliminar un sistema modular, realice los pasos siguientes:

1. En la consola OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de sistemas modulares**.
2. Seleccione los sistemas modulares y haga clic en **Eliminar**.

Vistas en OMIMSSC

Vea todos los dispositivos descubiertos en OMIMSSC en la página **Configuración e implementación**, junto con la información de su inventario de hardware y firmware. Además, vea todos los trabajos con estado en la página **Centro de trabajos y registros**.

Temas:

- [Iniviar vista de servidor](#)
- [Iniciar Vista de sistemas modulares](#)
- [Iniciar Vista de clúster](#)
- [Iniciar la consola iDRAC](#)
- [Iniciar el centro de mantenimiento](#)
- [Abrir el centro de trabajos y registros](#)

Iniviar vista de servidor

La página **Vista de servidor** enumera todos los servidores host y los servidores sin asignar detectados en OMIMSSC en las pestañas **Servidores sin asignar** y **Hosts**.

En la pestaña **Servidores sin asignar**, vea la dirección IP de iDRAC, la etiqueta de servicio, el modelo, la generación, la velocidad del procesador, la memoria del servidor, el estado de compatibilidad de la plantilla para una Plantilla operativa asignada, la etiqueta de servicio del sistema modular si se trata de un servidor modular y la información de compatibilidad del hardware. Si pasa el cursor por encima de la columna **Compatibilidad de hardware**, puede ver las versiones de BIOS, iDRAC, LC y los paquetes de controlador del dispositivo. Para obtener más información acerca de la compatibilidad de hardware, consulte [Acerca de las actualizaciones de firmware](#).

En la pestaña **Hosts**, vea el nombre del host, la dirección IP de iDRAC, la etiqueta de servicio, el modelo, la generación, la velocidad del procesador, la memoria del servidor, la etiqueta de servicio del sistema modular si se trata de un servidor modular, el nombre de dominio calificado (FQDN) si el servidor forma parte de un clúster, el estado de compatibilidad de la plantilla para una Plantilla operativa asignada y la información de compatibilidad del hardware. Si pasa el cursor por encima de la columna **Compatibilidad de hardware**, puede ver las versiones de BIOS, iDRAC, LC y los paquetes de controlador del dispositivo. Para obtener más información acerca de la compatibilidad de hardware, consulte [Acerca de las actualizaciones de firmware](#).

En la página **Vista de servidor**, puede realizar las siguientes tareas:

- [Descubrir servidores](#)
- Vea información actualizada mediante la actualización de la página.
- [Eliminar servidores desde OMIMSSC](#).
- [Sincronizarse con la consola Microsoft inscrita](#).
- [Resolver errores de sincronización](#).
- [Asignar una Plantilla operativa y evaluar la compatibilidad de la Plantilla operativa](#).
- [Implementar una plantilla operativa](#)
- Correlacionar servidores con un grupo de clúster y el sistema modular al que pertenece el servidor.
- [Iniciar consola del iDRAC](#)

Para ver los servidores:

1. En la extensión de la consola de OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de servidor**.
2. Para ver servidores de bajo nivel, haga clic en la pestaña **Servidores sin asignar**.
3. Para ver servidores host, haga clic en la pestaña **Hosts**.
 - a. Para ver grupos de hosts en formato anidado según su agrupación en SCCM o SCVMM, haga clic en el menú desplegable **Seleccionar hosts de consola**.

El menú desplegable **Seleccionar hosts de consola** muestra todos los grupos de host presentes en SCCM junto con un nombre interno de grupo. Si selecciona el nombre interno de grupo, se muestran todos los hosts detectados y administrados en SCCM y OMIMSSC.

Después de descubrir servidores, tenga en cuenta los siguientes puntos:

- La columna **Plantilla operativa** se muestra como **No asignada** después de descubrir los servidores. Para actualizar el firmware e implementar el sistema operativo en estos servidores, asigne e implemente Plantilla operativa. Para obtener más información, consulte [Administrar Plantilla operativa](#).
- Los servidores detectados se agregan a grupos predefinidos en OMIMSSC. Puede crear grupos de actualización personalizados según sus requisitos funcionales. Para obtener más información, consulte [Acerca de los grupos de actualización](#).
- Al iniciar sesión en OMIMSSC como un administrador delegado, puede ver todos los servidores host y los servidores sin asignar que no son específicos de este usuario. Por lo tanto, asegúrese de contar con los privilegios necesarios antes de realizar cualquier operación en los servidores.
- Si hay varias consolas Microsoft inscritas en OMIMSSC, entonces los servidores host son específicos para la consola Microsoft en la cual se administran. Los servidores sin asignar son comunes para todas las consolas.

Iniciar Vista de sistemas modulares

La página **Vista de sistemas modulares** muestra todos los sistemas modulares descubiertos en OMIMSSC.

Vea la dirección IP de la CMC, la etiqueta de servicio, el modelo, la versión de firmware, el estado de compatibilidad de plantilla de un sistema modular para una Plantilla operativa asignada, la cantidad de servidores, los módulos de entrada/salida (E/S) y los dispositivos de almacenamiento presentes en dicho sistema modular. Configure el hardware y actualice el firmware del sistema modular implementando la Plantilla operativa.

Puede realizar las siguientes tareas en la página **Vista de sistemas modulares**:

- [Descubrir sistemas modulares mediante el descubrimiento manual](#)
- Eliminar un sistema modular
- Ver la información de inventario más reciente; para ello, actualice la página.
- [Asignar una Plantilla operativa a un sistema modular](#)
- [Implementar una Plantilla operativa en un sistema modular](#)
- [Ver módulos de E/S](#)
- [Iniciar módulos de E/S](#)

Para ver el sistema modular detectado en OMIMSSC:

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de sistemas modulares**. Se muestran todos los nombres de modelo de los sistemas modulares descubiertos.
2. Para ver un sistema modular en específico, haga clic en un nombre de modelo en **Vista de sistemas modulares**. Todos los sistemas modulares de ese modelo se muestran con su etiqueta de servicio.
3. Para ver todos los dispositivos presentes en ese sistema modular, haga clic en la etiqueta de servicio. Se muestran todos los servidores, los módulos de entrada/salida y los dispositivos de almacenamiento junto con sus detalles.

 **NOTA:** Solamente después de realizar un descubrimiento exhaustivo de un sistema modular, aparecen todos los dispositivos en el sistema modular y su información.

- De manera predeterminada, se muestra la pestaña **Servidores**. Aparecen todos los servidores descubiertos en este sistema modular.
- Para ver todos los módulos de entrada/salida presentes en un sistema modular, haga clic en la pestaña **Módulos de E/S**.
- Para ver todos los dispositivos de almacenamiento presentes en el sistema modular, haga clic en la pestaña **Dispositivos de almacenamiento**.

Luego de descubrir sistemas modulares, tenga en cuenta los siguientes puntos:

- La columna **Plantilla operativa** aparece como **No asignada** después de descubrir los sistemas modulares. Para actualizar el firmware e implementar el sistema operativo en estos sistemas modulares, asigne e implemente las Plantilla operativa. Para obtener más información, consulte [Administrar Plantilla operativa](#).
- Vea el conteo de entrada/salida, dispositivos de almacenamiento y servidores presentes en sistemas modulares después de un descubrimiento ligero. Realice un descubrimiento exhaustivo para ver más detalles acerca de los componentes en un sistema modular.

Iniciar la consola OpenManage Enterprise Modular

Para iniciar la consola OpenManage Enterprise Modular, realice los pasos siguientes:

1. En OMIMSSC, expanda **Configuración e implementación** y haga clic en **Sistemas modulares**.
2. Haga clic en la **IP de dispositivo** del sistema modular.

Módulos de entrada/salida

Se muestran todos los módulos de entrada/salida de red, junto con su dirección IP, etiqueta de servicio, tipo de entrada/salida, modelo, versión de firmware e información de ranura.

Ejecute la consola de módulos de E/S desde la página Módulos de entrada/salida.

Para ver información acerca de los módulos de entrada/salida, realice los pasos siguientes:

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de sistemas modulares**. Expanda la **vista de sistemas modulares** y haga clic en la etiqueta de servicio.
Se muestran todas las etiquetas de servicio de ese modelo.
2. Para ver el módulo de entrada/salida, haga clic en la pestaña **Módulos de E/S**.

Iniciar consola de módulos de entrada/salida

Para iniciar la consola Módulo de Entrada/Salida, realice los pasos siguientes:

1. En OMIMSSC, expanda **Configuración e implementación** y haga clic en **Vista de sistemas modulares**. Expande el modelo a nivel de dispositivos individuales.
Se muestran todos los dispositivos con ese modelo.
2. Haga clic en la pestaña **Módulos de E/S**.
3. Haga clic en la **dirección IP** del dispositivo.

Iniciar Vista de clúster

En la página **Vista de clúster**, se indican todos los clústeres descubiertos en OMIMSSC. Vea el nombre de dominio calificado (FQDN) del clúster, la etiqueta de servicio y la cantidad de servidores presentes en ese clúster. Además, cree un switch lógico para clústeres y, luego, cree clústeres Storage Spaces Direct con la Plantilla operativa predefinida.

Puede realizar las siguientes tareas en la página **Vista de clúster**:

- [Crear un switch lógico](#) (solo para usuarios SCVMM 2016 y 2019)
- [Crear clústeres de Storage Spaces Direct](#) (solo para usuarios SCVMM 2016 y 2019)
- [Inicio de la consola de iDRAC](#)
- Para ver los últimos clústeres descubiertos, actualice la página.

Para ver grupos de clústeres descubiertos en OMIMSSC:

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de clúster**.
Todos los diferentes tipos de clústeres aparecen agrupados.
2. Para ver información acerca de los tipos específicos de clústeres, expanda el tipo de clúster.
Todos los clústeres de este tipo aparecen en el panel izquierdo.
3. Para ver los servidores presentes en un clúster, haga clic en un nombre de clúster.

Iniciar la consola iDRAC

Para iniciar la consola de iDRAC, realice el paso siguiente:

En OMIMSSC, expanda **Configuración e implementación** y seleccione una de las siguientes opciones:

- Haga clic en **Vista de servidor**. Según el servidor (si se trata de un host o un servidor sin asignar), haga clic en la pestaña **Servidores sin asignar** o **Hosts**; luego, haga clic en la dirección **IP de iDRAC** del servidor.

La pestaña **Servidores sin asignar** se muestra de manera predeterminada.

Para ver la pestaña Hosts, haga clic en **Hosts**.

- Haga clic en **Vista de clúster**. Expanda el tipo de clúster y expanda el grupo de clúster a nivel de servidor. Aparece la pestaña **Servidor**.

Iniciar el centro de mantenimiento

En la página **Centro de mantenimiento**, se muestran todos los dispositivos descubiertos en grupos y los recursos necesarios para el mantenimiento de dispositivos en OMIMSSC. Para ver los grupos de clústeres S2D en la página **Centro de mantenimiento**, asegúrese de haber seleccionado **Todos los grupos de actualización** en el menú desplegable **Grupo de actualización**. Vea el inventario de firmware del dispositivo, administre los dispositivos actualizando su firmware según las recomendaciones, revierta el servidor a un estado anterior en caso de fallas, ingrese la misma configuración de un componente antiguo a un componente de reemplazo y exporte registros del servidor para solucionar problemas. En la página **Configuración de actualización**, vea todos los orígenes de actualización, el sondeo y las notificaciones de las actualizaciones más recientes desde el origen de actualización predeterminado y actualice grupos de dispositivos que requieran la misma administración y todos los almacenes de protección necesarios para las configuraciones de servidor.

NOTA: De manera predeterminada, OMIMSSC incluye un archivo de catálogo que muestra una versión anterior del informe de comparación para el origen de actualización predefinido de FTP, HTTP y HTTPS. Por lo tanto, descargue el catálogo más reciente para mostrar el último informe de comparación. Para descargar el catálogo más reciente, edite y guarde los orígenes de actualización de FTP, HTTP y HTTPS.

NOTA: La versión de base de un componente específico de un dispositivo se marca como no disponible si la actualización no está presente en el catálogo de origen de actualizaciones seleccionado.

Puede realizar las siguientes tareas en la página **Centro de mantenimiento**:

- [Crear un origen de actualización](#)
- [Establecer la frecuencia de sondeo](#)
- Seleccionar grupos de actualización predefinidos o [crear grupos de actualización personalizados](#).
- [Ver y actualizar el inventario de firmware](#)
- [Actualizar y revertir versiones de firmware mediante el método Ejecutar actualización](#)
- [Crear almacenes de protección](#)
- [Exportar perfiles de servidor](#)
- [Importar perfiles de servidor](#)
- [Exportación de inventario](#)

Para ver la página **Centro de mantenimiento**:

En OMIMSSC, haga clic en OMIMSSC.

Se muestra la página **Centro de mantenimiento**.

Abrir el centro de trabajos y registros

Vea información acerca de los trabajos iniciados en OMIMSSC, junto con el estado de progreso del trabajo y su subtarea. Además, puede filtrar y ver trabajos para una categoría de trabajo específica.

Puede ver los trabajos que se inician desde OMIMSSC, en el portal de administración de OMIMSSC y en la extensión de consola de OMIMSSC.

- Portal de administración de OMIMSSC: muestra los trabajos que se inician desde todas las consolas y los usuarios de OMIMSSC
- Consola OMIMSSC: muestra los trabajos específicos de un usuario y una consola

Los nombres de los trabajos se pueden generar por el sistema, o bien los usuarios pueden ingresarlos, mientras que el nombre de las subtareas es la dirección IP o el nombre de host de los sistemas administrados. Expanda la subtarea para ver los registros de actividad para ese trabajo. Los trabajos se clasifican en cuatro grupos:

- **En ejecución:** muestra todos los trabajos que actualmente están en ejecución y en el estado "en curso".
- **Historial:** muestra todos los trabajos que se ejecutaron anteriormente con su estado de tarea.
- **Programado:** muestra todos los trabajos programados para una fecha y hora a futuro. Además, puede cancelar estos trabajos programados.

- **Registros genéricos:** muestra mensajes de registro comunes y específicos de dispositivos de OMIMSSC que no son específicos de una tarea, además de otras actividades. Todos los trabajos se muestran con un nombre de usuario y un FQDN de consola desde el punto en el cual se iniciaron.
 - **Mensajes de registro de dispositivo:** muestra todos los mensajes de registro específicos de dispositivos de OMIMSSC, como el reinicio del dispositivo de OMIMSSC. Solo puede ver esta categoría de mensajes desde el portal de administración de OMIMSSC.
 - **Mensajes de registro genérico:** muestra mensajes de registro que son comunes entre distintas categorías de trabajo, las cuales se enumeran en las pestañas **En ejecución**, **Historial** y **Programado**. Estos registros son específicos para una consola y un usuario.

Por ejemplo, si una tarea de actualización de firmware de un grupo de servidores se encuentra en progreso, la pestaña muestra los mensajes de registro que pertenecen a la creación del repositorio de Server Update Utility (SUU) para ese trabajo.

Los diferentes estados de un trabajo definido en OMIMSSC son los siguientes:

- **Cancelado:** el trabajo se canceló manualmente o después de reiniciar el dispositivo de OMIMSSC.
 - **Finalizado:** el trabajo se completó correctamente.
 - **Error:** el trabajo no se completó correctamente.
 - **En curso:** el trabajo se está ejecutando.
 - **Programado:** el trabajo se programó para una fecha y hora a futuro.
-  **NOTA:** Si se envían varios trabajos al mismo tiempo y al mismo dispositivo, los trabajos fallan. Por lo tanto, asegúrese de programar trabajos para el mismo dispositivo en diferentes momentos.
- **En espera:** el trabajo está en una línea de espera.
 - **Programación recurrente:** el trabajo está programado a intervalos regulares.

1. En OMIMSSC, haga clic en **Centro de trabajos y registros**.

2. Para ver una categoría específica de trabajos, como **Programado**, **Historial** o **Genérico**, haga clic en la pestaña correspondiente.

Expandir un trabajo para ver todos los dispositivos incluidos en él. Siga expandiendo para ver los mensajes de registro de ese trabajo.

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

3. (Opcional) Aplique filtros para ver diferentes grupos de trabajos y el estado del trabajo en la columna **Estado**.

Administrar Plantilla operativa

Las Plantilla operativa contienen la configuración completa de los dispositivos y se utilizan para implementar un sistema operativo y actualizar el firmware para servidores PowerEdge y sistemas modulares en un entorno de Microsoft.

La Plantilla operativa replica el hardware y el firmware de un servidor de referencia (servidor dorado) en varios otros servidores durante el aprovisionamiento de sistemas operativos. Contiene componentes de firmware, hardware y sistema operativo con su atributo establecido en el valor actual del servidor de referencia. Estos valores se pueden modificar antes de aplicar esta plantilla en los dispositivos. Además, puede comprobar el estado de compatibilidad de una Plantilla operativa asignada y ver el informe de compatibilidad en una página de resumen.

Solo se recuperan estos componentes disponibles en el servidor de referencia y se muestran de forma dinámica como componentes de Plantilla operativa. Por ejemplo, si el servidor no tiene un componente de FC, este no aparece en la Plantilla operativa.

Para obtener más información acerca del servidor de referencia y el sistema modular de referencia, consulte [Acerca de la configuración del servidor de referencia](#) y [Acerca de la configuración del sistema modular de referencia](#).

En la siguiente tabla, se describen los componentes que se enumeran en la Plantilla operativa y las capacidades de visualización e implementación de cada componente:

Tabla 7. Funcionalidad de la Plantilla operativa

Componente	Implementar configuración	Actualización del firmware	Ver configuración	Estado de compatibilidad 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	Sí	-	No	-
RHEL	Sí	-	No	-
ESXI	Sí	-	No	-
Módulo de administración	Sí	Sí	Sí	Sí

Temas:

- [Plantilla operativa predefinidas](#)
- [Acerca de la configuración de un servidor de referencia](#)
- [Crear una Plantilla operativa a partir de servidores de referencia](#)
- [Crear una Plantilla operativa a partir de sistemas modulares de referencia](#)
- [Visualizar una Plantilla operativa](#)
- [Modificar una Plantilla operativa](#)
- [Configurar valores específicos del sistema \(valores de pool\) mediante una plantilla operativa en varios servidores](#)
- [Eliminar una Plantilla operativa](#)
- [Asignar una Plantilla operativa y evaluar la compatibilidad de Plantilla operativa para los servidores](#)
- [Implementar una Plantilla operativa en servidores](#)
- [Asignar una Plantilla operativa a sistemas modulares](#)
- [Implementar Plantilla operativa para un sistema modular](#)
- [Cancelar asignación de Plantilla operativa](#)
- [Acerca de la configuración del sistema modular de referencia](#)

Plantilla operativa predefinidas

Las plantillas predefinidas disponen de todas las configuraciones necesarias para crear clústeres de Storage Spaces Direct o Windows Server definido por software (WSSD). OMIMSSC OMIMSSC admite la creación de clústeres en los modelos de nodo Storage Spaces Direct Ready R740XD, R740XD2 y R640 junto con sus adaptadores de red específicos.

Tabla 8. Lista de Plantilla operativa predefinidas

Nombre de Plantilla operativa	Descripción
R740XD_Mellanox_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R740XD que cuenten con tarjeta Mellanox.
R740XD2_Mellanox_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R740XD2 que cuenten con tarjeta Mellanox.
R740XD_QLogic_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R740XD que cuenten con tarjeta QLogic.
R740XD2_QLogic_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R740XD2 que cuenten con tarjeta QLogic.
R640_Mellanox_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R640 que cuenten con tarjeta Mellanox.
R640_QLogic_S2D_Template	Utilice esta plantilla para los modelos de nodo Storage Spaces Direct Ready R640 que cuenten con tarjeta QLogic.

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

- Las plantillas predefinidas solo están disponibles para sistemas de administración que ejecuten SCVMM 2016 y 2019.
- La plantilla Storage Spaces Direct predefinida muestra una tarjeta NIC en la ranura 1. Sin embargo, mientras se implementa la Plantilla operativa, la configuración del NIC se aplica en la ranura derecha. Además, si hay varias tarjetas NIC en el dispositivo, todas las tarjetas NIC adquieren la misma configuración especificada en la Plantilla operativa.

Acerca de la configuración de un servidor de referencia

Se denomina configuración de servidor de referencia a una configuración de servidor con una secuencia de arranque preferida y una configuración BIOS, RAID y hardware, atributos de actualización de firmware y parámetros de sistema operativo que son idealmente aptos para una organización.

Descubra un servidor de referencia, capture la configuración de servidor de referencia en una Plantilla operativa y replíquela a varios servidores distintos con la misma configuración de hardware.

Crear una Plantilla operativa a partir de servidores de referencia

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

- Descubra un servidor de referencia mediante la función **Descubrimiento**. Para obtener más información acerca de cómo descubrir servidores, consulte [Descubrir servidores mediante el descubrimiento manual](#).
- Para usuarios de SCCM:
 - Cree una secuencia de tareas. Para obtener más información, consulte [Crear una secuencia de tareas](#).
 - Para implementar un sistema operativo distinto a Windows, debe tener un perfil de credencial de tipo dispositivo. Para obtener más información, consulte [Crear un perfil de credencial](#).
- Para usuarios de SCVMM:
 - Cree un perfil de hipervisor. Para obtener información acerca de cómo crear un perfil de hipervisor, consulte [Crear perfil de hipervisor](#).

- Para implementar Windows, debe tener un perfil de credencial de tipo dispositivo. Para obtener más información, consulte [Crear un perfil de credencial](#).
- Si no utiliza el origen de actualización predeterminado, entonces cree un origen de actualización. Para obtener más información, consulte [Crear un origen de actualización](#).

Puede crear una Plantilla operativa mediante la captura de la configuración del servidor de referencia. Después de capturar la configuración, puede guardar directamente la plantilla o editar los atributos del origen de actualización, la configuración de hardware y el componente de Windows según sus necesidades. Ahora puede guardar la plantilla, la cual puede utilizar en servidores PowerEdge homogéneos.

1. En OMIMSSC, realice alguno de los siguientes pasos para abrir una Plantilla operativa:
 - En el panel de OMIMSSC, haga clic en **Crear plantilla operativa**.
 - En el panel de navegación, haga clic en **Perfiles > Plantilla operativa** y, luego, en **Crear**.

Aparece el asistente **Plantilla operativa**.

2. Ingrese un nombre y una descripción para la plantilla.
3. Seleccione el tipo de dispositivo, ingrese la dirección IP del dispositivo de referencia y, luego, haga clic en **Siguiente**.

NOTA: Puede capturar la configuración del servidor de referencia con iDRAC 2.0 y posterior.

4. En **Componentes del dispositivo**, haga clic en un componente para ver los atributos disponibles y sus valores.

A continuación, se enumeran los componentes:

- Actualización del firmware
- Componentes de hardware, los cuales son RAID, NIC y BIOS.

NOTA: En el componente **iDRAC integrado 1**, verá los siguientes privilegios y sus valores para el atributo **Privilegio de usuario administrador**.

Tabla 9. Tabla de valores de privilegio

Valor	Privilegio
1	Inicio de sesión
2	Configurar
4	Configurar usuarios
8	Registros
16	Control del sistema
32	Acceder a la consola virtual
64	Acceder a los medios virtuales
128	Operaciones del sistema
256	Depuración
499	Privilegios de operador

- Sistema operativo: seleccione Windows, ESXi o RHEL.

5. Utilice la barra de desplazamiento horizontal para localizar un componente. Seleccione el componente, expanda un grupo y, luego, edite sus valores de atributo. Utilice la barra de desplazamiento vertical para editar los grupos y atributos de un componente.
6. Seleccione la casilla de verificación en cada uno de los componentes, ya que las configuraciones de los componentes seleccionados se aplican en el dispositivo administrado cuando se aplica la Plantilla operativa. Sin embargo, todas las configuraciones del dispositivo de referencia se capturan y guardan en la plantilla.

NOTA: Sin importar que selección realice en la casilla de verificación de cada componente, todas las configuraciones se capturan en la plantilla.

En el componente **Sistema operativo**, realice los pasos que se indican en cualquiera de las opciones siguientes, según sus requisitos:

- Para implementar el sistema operativo Windows en SCCM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCCM](#).

- Para implementar el sistema operativo Windows en SCVMM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCVMM](#).
- OMIMSSC
- Para implementar un sistema operativo distinto a Windows, consulte [Componente distinto a Windows para las extensiones de la consola de OMIMSSC](#).

7. Para guardar el perfil, haga clic en **Completar**.

Componente del SO Windows para la extensión de consola de OMIMSSC para SCCM

Cuando cree o edite una Plantilla operativa para un servidor, realice los siguientes pasos en un componente Windows:

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

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

Para obtener más información acerca de la secuencia de tareas, consulte [Secuencia de tareas](#).

2. Seleccione una de las siguientes opciones para el **método de implementación**:

- **Arrancar en ISO de red:** reinicia la ISO especificada.
- **Colocar ISO en vFlash y reiniciar:** descarga la imagen ISO en vFlash y reinicia.
- **Reiniciar en vFlash:** reinicia en vFlash. Asegúrese de que la imagen ISO esté presente en vFlash.

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

3. (Opcional) Para utilizar la imagen presente en el recurso compartido de red, seleccione la opción **Utilizar ISO de red como alternativa**.
4. Ingrese un archivo de imagen de medios de arranque LC.
5. Seleccione los controladores necesarios para el sistema operativo.

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

Cuando cree o edite una Plantilla operativa para un servidor, realice los siguientes pasos en un componente Windows:

Seleccione **Perfil de hipervisor**, **Perfil de credencial** y **Origen de IP de servidor**.

NOTA: **Nombre de host** y **NIC de administración de servidor** siempre son valores de pool. En el caso de una NIC de administración de servidores, proporcione la dirección MAC del puerto de red a través del cual desea que el sistema operativo se comunique con SCVMM.

Si selecciona **Origen de IP de servidor** como **Estático**, entonces asegúrese de haber configurado la red lógica en SCVMM y que los siguientes campos sean valores de pool:

- **Red lógica de consola**
- **Subred IP**
- **Dirección IP estática**

Componente no perteneciente a Windows para las extensiones de consola de OMIMSSC

Cuando cree o edite una Plantilla operativa para un servidor, realice los siguientes pasos en un componente no perteneciente a Windows:

Seleccione un sistema operativo distinto a Windows, la versión del sistema operativo, el tipo de carpeta de recurso compartido, el nombre del archivo ISO, la ubicación del archivo ISO y la contraseña de la cuenta root del sistema operativo.

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

Nombre de host es un valor de pool y si desactiva la opción DHCP, entonces los siguientes campos serán valores de pool:

- **Dirección IP**
- **Máscara de subred**
- **Puerta de enlace predeterminada**
- **DNS primario**
- **DNS secundario**

NOTA: Los tipos de recurso compartido NFS (Sistema de archivos de red) y CIFS (Sistema de archivos de Internet común) son compatibles para la implementación de un sistema operativo distinto a Windows.

Crear una Plantilla operativa a partir de sistemas modulares de referencia

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

- Descubra un sistema modular mediante la función **Descubrimiento**. Para obtener más información acerca de cómo descubrir sistemas modulares, consulte [Descubrir sistemas modulares mediante el descubrimiento manual](#).
- Si no utiliza el origen de actualización predeterminado, entonces cree un origen de actualización. Para obtener más información, consulte [Crear un origen de actualización](#).

Puede crear una Plantilla operativa capturando la configuración de los sistemas modulares de referencia. Después de capturar la configuración, puede guardar la plantilla directamente, o bien editar los atributos del origen de actualización y la configuración de hardware según sus requisitos. Ahora puede guardar la plantilla, la cual puede utilizar para configurar otros sistemas modulares del mismo modelo.

NOTA: Si desea configurar usuarios de Active Directory (AD) en otros dispositivos MX7000, asegúrese de crear una Plantilla operativa desde un sistema modular MX7000 en el que todos los usuarios de AD estén configurados.

NOTA: Por motivos de seguridad, las contraseñas de cuenta de usuario no se capturan en una plantilla operativa desde un sistema modular de referencia. Edite la Plantilla operativa para agregar una nueva cuenta de usuario y contraseña; luego, aplique la Plantilla operativa en los sistemas modulares administrados. De otro modo, puede aplicar la Plantilla operativa sin realizar cambios en las cuentas de usuario. Entonces, las mismas contraseñas que se utilizan en el sistema modular de referencia se aplican al sistema modular administrado.

1. En OMIMSSC, realice alguno de los siguientes pasos para abrir una Plantilla operativa:

- En el panel de OMIMSSC, haga clic en **Crear plantilla operativa**.
- En el panel de navegación, haga clic en **Perfiles > Plantilla operativa** y, luego, en **Crear**.

Aparece el asistente **Plantilla operativa**.

2. Ingrese un nombre y una descripción para la plantilla.

3. En **Componentes del dispositivo**, haga clic en un componente para ver los atributos disponibles y sus valores.

A continuación, se enumeran los componentes:

- Actualización del firmware
- Módulo de administración integrado

NOTA: Asegúrese de que el atributo **Servidor web** está seleccionado. Si este componente no está activado, entonces no podrá acceder a los sistemas modulares MX7000 mediante OMIMSSC después de implementar la Plantilla operativa.

NOTA: Para **Configuración de SNMP** y **Configuración del registro del sistema**, asegúrese de seleccionar las cuatro configuraciones disponibles en cada atributo para aplicarlas en los sistemas administrados.

4. Utilice la barra de desplazamiento horizontal para localizar un componente. Seleccione el componente, expanda un grupo y, luego, edite sus valores de atributo. Utilice la barra de desplazamiento vertical para editar los grupos y atributos de un componente.

5. Seleccione la casilla de verificación en cada uno de los componentes, ya que las configuraciones de los componentes seleccionados se aplican en el dispositivo administrado cuando se aplica la Plantilla operativa. Sin embargo, todas las configuraciones del dispositivo de referencia se capturan y guardan en la plantilla.

6. Para guardar el perfil, haga clic en **Completar**.

Visualizar una Plantilla operativa

Para ver las Plantilla operativa creadas:

En la consola de OMIMSSC, haga clic en **Perfiles y plantillas** y, luego, en **Plantilla operativa**. Aquí se incluyen todas las plantillas que se crean.

Modificar una Plantilla operativa

Puede modificar el origen de actualización, las configuraciones de hardware y el sistema operativo de una plantilla operativa.

Tenga en cuenta lo siguiente antes de modificar una Plantilla operativa:

- Los valores de algunos atributos dependen de los valores de otros atributos. Cuando cambie manualmente los valores de un atributo, asegúrese de cambiar también los atributos interdependientes. Si no cambia estos valores interdependientes según corresponda, entonces la aplicación de las configuraciones de hardware puede fallar.
- La creación de una Plantilla operativa recupera todas las configuraciones de hardware del servidor de referencia especificado, las cuales pueden contener atributos específicos del sistema. Por ejemplo, una dirección IPv4 estática o una etiqueta de activo. Para configurar atributos específicos del sistema, consulte [Configurar valores específicos del sistema mediante una Plantilla operativa](#)
- Los atributos de la Plantilla operativa se asignan con los valores actuales del servidor de referencia. Las Plantilla operativa también muestran otros valores aplicables para los atributos.
- Para modificar Plantilla operativa predefinidas y Plantilla operativa personalizadas, realice los siguientes pasos:

i **NOTA:** (Solo para usuarios y servidores de SCVMM) Todos los atributos obligatorios (los atributos obligatorios que se capturan en la plantilla operativa son los atributos recomendados por Dell EMC para el clúster S2D) requeridos para Storage Spaces Direct son atributos de solo lectura en la plantilla predefinida de Storage Spaces Direct. Sin embargo, puede editar el nombre de la plantilla, los componentes del sistema operativo y los atributos no obligatorios de configuración de hardware

1. Seleccione la plantilla que desea modificar y haga clic en **Editar**.
Se muestra la página Plantilla operativa.
2. (Opcional) Ingrese el nombre y la descripción para la plantilla y, luego, haga clic en **Siguiente**.
3. Para ver los atributos disponibles y sus valores en **Componentes de dispositivo**, haga clic en un componente.
4. Modifique los valores de los atributos disponibles.

i **NOTA:** Seleccione la casilla de verificación en cada uno de los componentes, debido a que solo las configuraciones de los componentes seleccionados se aplican en el sistema administrado cuando se aplica la Plantilla operativa.

i **NOTA:** Cuando edita una Plantilla operativa, muy pocos atributos de componente de la interfaz de controladora host avanzada (AHCI) de solo lectura aparecen como editables. Sin embargo, cuando se establecen estos atributos de solo lectura y se implementa la Plantilla operativa, no se realizan cambios en el dispositivo.

- Para los sistemas modulares MX7000:
 - Las configuraciones se aplican solo si todos los atributos de un grupo están seleccionados. Por lo tanto, asegúrese de seleccionar todos los atributos de un grupo, incluso si desea cambiar uno de los atributos en el grupo.
 - Para agregar un nuevo usuario mediante una Plantilla operativa, seleccione todos los atributos de los usuarios existentes que se exportaron durante la captura de la Plantilla operativa, seleccione los grupos de usuarios agregados recientemente y guarde la Plantilla operativa.
 - Para proporcionar los valores de zona horaria, consulte el [Apéndice](#).
5. Para el componente del sistema operativo, realice una de las siguientes tareas según sus necesidades:
 - Para implementar el sistema operativo Windows en SCCM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCCM](#).
 - Para implementar el sistema operativo Windows en SCVMM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCVMM](#).
 - OMIMSSC
 - Para implementar un sistema operativo distinto a Windows, consulte [Componente distinto a Windows para las extensiones de la consola de OMIMSSC](#).
 6. Para guardar el perfil, haga clic en **Completar**.

Configurar valores específicos del sistema (valores de pool) mediante una plantilla operativa en varios servidores

OMIMSSC recuperará la configuración actual del dispositivo. Los atributos específicos de un sistema, como la dirección IPv4 estática para iDRAC, se mostrarán como un valor de pool en la plantilla operativa. De manera predeterminada, los atributos de valor de pool que son atributos dependientes no se seleccionan y los otros atributos están seleccionados de forma predeterminada.

1. Seleccione la plantilla que desea modificar y haga clic en **Editar**.
Se muestra la página **Plantilla operativa**.
2. (Opcional) Ingrese el nombre y la descripción para la plantilla y, luego, haga clic en **Siguiente**.
3. Para ver los atributos disponibles y sus valores en **Componentes de dispositivo**, haga clic en un componente.
4. Expanda el **grupo de atributos**. Si el valor del atributo es Valor de pool, se identifica el atributo como un atributo específico del sistema.
5. Se pueden ingresar estos atributos específicos del sistema en varios servidores a través de un archivo .CSV mediante la opción **Exportar atributos de pool** durante la implementación de una plantilla operativa; consulte [Implementar una plantilla operativa en servidores](#).
6. Si no desea aplicar estos atributos específicos del sistema, identifique estos atributos (que se mencionan en el paso 3) y anule su selección durante la edición de la plantilla operativa.

Eliminar una Plantilla operativa

Para eliminar una Plantilla operativa, lleve a cabo los pasos siguientes:

Antes de eliminar una Plantilla operativa, verifique lo siguiente:

- La Plantilla operativa seleccionada no está asociada a ningún servidor o sistema modular. Si está asociada a un dispositivo, entonces cancele la asignación de la plantilla y, luego, elimine la plantilla.
- No se está ejecutando ningún trabajo asociado a la Plantilla operativa.
- No ha seleccionado una Plantilla operativa predefinida, puesto que no puede eliminar una plantilla predefinida.
- Los pasos para eliminar cualquier tipo de Plantilla operativa son los mismos.

Seleccione las plantillas que desea eliminar y haga clic en **Eliminar**. Para confirmar, haga clic en **Sí**.

Asignar una Plantilla operativa y evaluar la compatibilidad de Plantilla operativa para los servidores

Asigne una Plantilla operativa a un servidor y evalúe la compatibilidad de la Plantilla operativa. Solo después de asignar una Plantilla operativa a un servidor, podrá ver el estado de compatibilidad de su Plantilla operativa. Para comparar la configuración de un servidor con una Plantilla operativa, asigne la plantilla a un servidor. Una vez que asigne una Plantilla operativa, se ejecuta el trabajo de compatibilidad y aparece el estado de la Plantilla operativa tras finalizar.

Para asignar una Plantilla operativa, lleve a cabo los pasos siguientes:

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de servidor**. Seleccione los servidores necesarios y haga clic en **Asignar plantilla operativa y evaluar compatibilidad**.
Aparece la página **Asignar Plantilla operativa y evaluar compatibilidad**.
2. Seleccione la plantilla en el menú desplegable **Plantilla operativa**, ingrese un nombre de trabajo y, luego, haga clic en **Asignar**.

El menú desplegable Plantilla operativa enumera las plantillas del mismo tipo que el de los dispositivos seleccionados en el paso anterior.

Si el dispositivo es compatible con la plantilla, entonces aparece una casilla de color **verde** con una marca de verificación.

Si la Plantilla operativa no se aplica correctamente en el dispositivo o si el componente de hardware en Plantilla operativa no está seleccionado, entonces aparece una casilla con el símbolo de **información**.

Si el dispositivo no es compatible con la plantilla, entonces aparece una casilla con el símbolo de **advertencia**. Únicamente si el dispositivo no es compatible con la Plantilla operativa asignada, puede ver un informe de resumen haciendo clic en el enlace del nombre de la plantilla. La página **Informe de resumen de compatibilidad de Plantilla operativa** muestra un informe de resumen de las diferencias entre la plantilla y el dispositivo.

Para ver un informe detallado, realice los pasos siguientes:

- a. Haga clic en **Ver compatibilidad detallada**. Aquí se muestran los componentes cuyos valores de atributos son distintos a los valores de la plantilla asignada. Los colores indican los diferentes estados de compatibilidad de la Plantilla operativa.
 - Símbolo de advertencia de color amarillo: incompatible. Indica que la configuración del dispositivo no coincide con los valores de plantilla.
 - Recuadro de color rojo: indica que el componente no está presente en el dispositivo.

Implementar una Plantilla operativa en servidores

Para implementar un sistema operativo en servidores administrados, asegúrese de tener instalado el artículo de KB 4093492 o una versión posterior en el sistema de administración y en la imagen del sistema operativo que utiliza para la implementación.

Puede implementar un sistema operativo Windows u otro distinto (ESXi y RHEL) implementando la Plantilla operativa asignada a los servidores.

i **NOTA:** Descargue e instale los controladores que correspondan desde Dell.com/support si aparece un ícono de advertencia amarillo en Administrador de dispositivos después de implementar el sistema operativo Windows 2016 o Windows 2019 en servidores de 12.ª generación.

i **NOTA:** La implementación de una plantilla operativa en servidores se bloquea si el modo de bloqueo está activado en los servidores.

i **NOTA:** Cuando implemente Windows en un dispositivo basado en UEFI, formatee el disco duro que incluye la partición de Windows mediante un sistema de archivos de la tabla de particiones GUID (GPT). Para obtener más información, consulte la sección [Particiones de disco duro basadas en UEFI/GPT](#) en la documentación de Microsoft.

1. En OMIMSSC, haga clic en **Configuración e implementación** y haga clic en **Vista de servidor**. Seleccione los servidores en los que desea implementar una plantilla y, luego, haga clic en **Implementar Plantilla operativa**. Aparecerá el asistente **Implementar Plantilla operativa**.

i **NOTA:** Si ve el símbolo del sistema *Press any key to boot to CD \ DVD* durante el arranque de medios de secuencia de tareas. Para obtener información sobre cómo quitar el símbolo del sistema y cómo arrancar automáticamente los medios de secuencia de tareas, consulte la sección [Instalación de Windows en una computadora basada en EFI](#) en la documentación de Microsoft.

2. (Opcional) Para exportar todos los atributos marcados como valores de pool en la plantilla seleccionada a un archivo .CSV, haga clic en **Exportar atributos de pool**; de lo contrario, vaya al paso 4.

Antes de exportar los valores de pool, agregue al sitio de intranet local la dirección IP del dispositivo de OMIMSSC en el que está instalada la extensión de consola de OMIMSSC.

3. Si exportó los valores de pool, ingrese valores para todos los atributos que se marcan como valores de pool en el archivo .CSV y guarde el archivo. En **Pool de valor de atributo**, seleccione este archivo para importarlo.

El formato de un archivo .CSV es `attribute-value-pool.csv` `attribute-value-pool.csv`

i **NOTA:** Asegúrese de seleccionar un archivo .CSV que tenga todos los atributos correspondientes y que no cambien ni la IP de iDRAC ni las credenciales de iDRAC debido a la plantilla, puesto que OMIMSSC deja de hacer seguimiento del trabajo después de que la IP de iDRAC o las credenciales de iDRAC cambian y se marca como fallido a pesar de que el trabajo se realice correctamente en iDRAC.

4. Ingrese un nombre de trabajo único y una descripción para el trabajo, y haga clic en **Implementar**.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Asignar una Plantilla operativa a sistemas modulares

Asigne una Plantilla operativa a un sistema modular y evalúe la compatibilidad de la Plantilla operativa. Esta operación compara la configuración de un sistema modular y una Plantilla operativa mediante la asignación de la plantilla seleccionada a un sistema modular. Después de asignar una Plantilla operativa, se ejecuta el trabajo de compatibilidad y aparece el estado de compatibilidad tras finalizar.

Para asignar una Plantilla operativa a sistemas modulares, realice los pasos siguientes:

1. En OMIMSSC, haga clic en **Configuración e implementación** y en **Vista de sistemas modulares**. Seleccione el sistema modular necesario y haga clic en **Asignar plantilla operativa**.

Aparece la página **Asignar Plantilla operativa**.

2. Seleccione la plantilla en el menú desplegable **Plantilla operativa**, ingrese un nombre de trabajo y, luego, haga clic en **Asignar**.

Si el dispositivo es compatible con la plantilla, entonces aparece una casilla de color **verde** con una marca de verificación.

Si la Plantilla operativa no se aplica correctamente en el dispositivo o si el componente de hardware en Plantilla operativa no está seleccionado, entonces aparece una casilla con el símbolo de **información**.

 **NOTA:** El estado de compatibilidad de la Plantilla operativa excluye los cambios realizados a los atributos de usuario.

Si el dispositivo no es compatible con la plantilla, entonces aparece una casilla con el símbolo de **advertencia**. Únicamente si el dispositivo no es compatible con la Plantilla operativa asignada, puede ver un informe de resumen haciendo clic en el enlace del nombre de la plantilla. La página **Informe de resumen de compatibilidad de Plantilla operativa** muestra un informe de resumen de las diferencias entre la plantilla y el dispositivo.

Para ver un informe detallado, realice los pasos siguientes:

- a. Haga clic en **Ver compatibilidad detallada**. Aquí se muestran los componentes cuyos valores de atributos son distintos a los valores de la plantilla asignada. Los colores indican los diferentes estados de compatibilidad de la Plantilla operativa.
 - Símbolo de advertencia de color amarillo: incompatible. Indica que la configuración del dispositivo no coincide con los valores de plantilla.
 - Recuadro de color rojo: indica que el componente no está presente en el dispositivo.

Implementar Plantilla operativa para un sistema modular

Puede configurar los componentes del sistema modular y actualizar las versiones de firmware del sistema modular mediante la implementación de la Plantilla operativa asignada.

 **NOTA:** En una administración de varios chasis (MCM), si el chasis principal está configurado con la opción **Propagación a los chasis miembros**, entonces la configuración y actualización del chasis principal y los chasis miembros desde OMIMSSC anulará los cambios realizados mediante la propagación.

1. En OMIMSSC, haga clic en **Configuración e implementación** y en **Vista de sistemas modulares**. Seleccione el sistema modular en el cual asignó la plantilla y, luego, haga clic en **Implementar Plantilla operativa**. Aparecerá el asistente **Implementar Plantilla operativa**.
2. (Opcional) Para exportar todos los atributos marcados como valores de pool en la plantilla seleccionada a un archivo .CSV, haga clic en **Exportar atributos de pool**; de lo contrario, vaya al paso 4.
3. Si exportó los valores de pool, ingrese valores para todos los atributos que se marcan como valores de pool en el archivo .CSV y guarde el archivo. En **Pool de valor de atributo**, seleccione este archivo para importarlo.

El formato de un archivo .CSV es `attribute-value-pool.csv` `attribute-value-pool.csv`

 **NOTA:** Asegúrese de seleccionar un archivo .CSV que tenga todos los atributos correspondientes y que no cambien la IP ni las credenciales de CMC debido a la plantilla, ya que OMIMSSC no realiza seguimiento al trabajo después de que cambia la IP o las credenciales de CMC.

4. Ingrese un nombre de trabajo único y una descripción para el trabajo, y haga clic en **Implementar**.

 **NOTA:** No existen atributos de valor de pool específicos de un sistema compatible para un sistema modular. Por lo tanto, no hay valores de pool para exportar.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Cancelar asignación de Plantilla operativa

1. En OMIMSSC, realice una de las siguientes tareas:
 - Haga clic en **Configuración e implementación** y haga clic en **Vista de servidor**.
 - Haga clic en **Configuración e implementación** y haga clic en **Vista de sistemas modulares**.Seleccione los dispositivos necesarios y haga clic en **Asignar plantilla operativa y evaluar compatibilidad**.
Aparece la página **Asignar Plantilla operativa y evaluar compatibilidad**.
2. Seleccione **Cancelar asignación** desde el menú desplegable **Plantilla operativa** y haga clic en **Asignar**.
La asignación de la Plantilla operativa se canceló en los dispositivos seleccionados.

Acerca de la configuración del sistema modular de referencia

Se denomina configuración del sistema modular de referencia o chasis de referencia a una configuración de sistema modular con una configuración de red preferida y una configuración de cuenta de usuario, seguridad y alertas que son idealmente aptos para una organización.

Descubra un sistema modular de referencia, capture su configuración en una Plantilla operativa y replíquela en distintos sistemas modulares de los mismos modelos.

Preparación para implementar un sistema operativo

Antes de implementar el sistema operativo Windows en los servidores administrados, actualice la imagen de WinPE y cree un archivo LC de medios de arranque para secuencia de tareas y un archivo ISO de medios de arranque para secuencia de tareas. Los pasos varían para los usuarios de consola SCCM y SCVMM. Para obtener más información, consulte la siguiente sección. Para implementar un sistema operativo distinto a Windows, recuerde los puntos mencionados en la sección [Preparación para implementar un SO distinto a Windows](#).

Temas:

- [Acerca de la imagen de WinPE](#)
- [Preparación para implementar el sistema operativo en la consola de SCCM](#)
- [Preparación para implementar un sistema operativo distinto a Windows](#)

Acerca de la imagen de WinPE

Se utiliza una imagen del entorno de preinstalación de Windows (WinPE) para implementar un sistema operativo. Utilice una imagen de WinPE actualizada para implementar un sistema operativo, pues es posible que la imagen de WinPE disponible en SCCM o SCVMM no tenga los controladores más recientes. Para crear una imagen de WinPE que tenga todos los controladores necesarios, actualice la imagen utilizando DTK. Asegúrese de que los paquetes de controladores relacionados con el sistema operativo correspondiente estén instalados en Lifecycle Controller.

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

Proporcionar un archivo WIM para SCCM

Copie el archivo `boot.wim` desde la siguiente ubicación `\\shareip\sms_sitecode\OSD\boot\x64\boot.wim` y, a continuación, péguelo en una carpeta de recurso compartido a la cual OMIMSSC pueda acceder. Por ejemplo, ubicación de la ruta compartida: `\\shareip\sharefolder\boot.wim`

Proporcionar un archivo WIM para SCVMM

La imagen base `boot.WimPE` que se proporciona para inyectar los controladores Dell críticos de arranque más recientes desde DTK se genera mediante la instalación de un servidor PXE en SCVMM.

1. Instale y configure la función WDS (Servidor de implementación de Windows) en un servidor y, luego, agregue el servidor PXE a SCVMM.
Para obtener información sobre cómo agregar la función WDS a un servidor y sobre cómo agregar un servidor PXE a SCVMM, consulte la sección [Aprovisionamiento de un host o clúster de Hyper-V desde computadoras vacías](#) de la documentación de Microsoft.
2. Copie el archivo `boot.wim` desde el servidor PXE presente en la siguiente ubicación: `C:\RemoteInstall\DCMgr\Boot\Windows\Images`. Luego, péguelo en una carpeta de recurso compartido a la cual OMIMSSC pueda acceder.
Por ejemplo, ubicación de la ruta compartida: `\\shareip\sharefolder\boot.wim`

WDS y el servidor PXE solo se requieren para generar la imagen `boot.in` basada en WinPE y no se debe usar en escenarios de implementación.

Extraer controladores de DTK

Un archivo de DTK contiene las versiones de firmware necesarias para los servidores en los que implementa los sistemas operativos.

To download DTK driver, launch <https://www.dell.com/support/> -> Browse all products -> Servers -> PowerEdge -> Select the server type < C Series, Modular, Rack, or Tower> -> Select the server model -> Search for the keyword **DTK** and download the required version.

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

1. Haga doble clic en el archivo ejecutable de DTK.
2. Para descomprimir los controladores de DTK, seleccione una carpeta. Por ejemplo, C:\DTK501.
3. Copie la carpeta descomprimida de DTK a una carpeta de recurso compartido. Por ejemplo, \\Shareip\sharefolder\DTK\DTK501

NOTA: Si está actualizando de SCVMM SP1 a SCVMM R2, actualice a Windows PowerShell 4.0. y cree una imagen ISO de WinPE.

Actualizar una imagen de WinPE

Se asigna un nombre de trabajo único a cada trabajo de actualización de WinPE.

1. En OMIMSSC, seleccione **Actualización de WinPE**. Se muestra la página **Actualización de WinPE**.
2. En **Fuente de imagen**, para **Ruta de imagen de WinPE personalizada**, ingrese la ruta de la imagen de WinPE junto con el nombre del archivo en el que se encuentra la imagen. Por ejemplo, \\Shareip\sharefolder\WIM\boot.wim.
3. En **Ruta de DTK**, para **Ruta de controladores de DTK**, ingrese la ubicación de los controladores de Dell EMC Deployment Toolkit. Por ejemplo, \\Shareip\sharefolder\DTK\DTK501
4. En **Archivo de salida**, para **Nombre de archivo ISO o WIM**, ingrese un nombre para el archivo junto con la ruta de archivo de recurso compartido donde se generará la imagen de WinPE.

Escriba uno de los tipos de archivos de salida:

- Archivo WIM para SCCM
- Archivo ISO para SCVMM

NOTA: La carpeta compartida debe estar en System Center Machine.

5. En la sección **Perfil de credencial**, para el espacio **Perfil de credenciales**, ingrese las credenciales que cuenten con acceso a la carpeta de recurso compartido en la cual se guarda la imagen de WinPE.
6. (Opcional) Para ver la lista de trabajos, seleccione **Ir a la lista de trabajos**. Se asigna un nombre de trabajo exclusivo a cada actualización del entorno de preinstalación de Windows (WinPE).
7. Haga clic en **Actualizar**. La imagen de WinPE con el nombre de archivo proporcionado en el paso anterior se crea en \\Shareip\sharefolder\WIM.

Preparación para implementar el sistema operativo en la consola de SCCM

Antes de implementar un sistema operativo en los servidores administrados descubiertos mediante OMIMSSC en la consola de SCCM, cree una secuencia de tareas personalizada o específica de Dell EMC, un archivo LC de medios de arranque y un archivo ISO de medios de arranque para secuencia de tareas.

Secuencia de tareas en SCCM

Una secuencia de tareas es una serie de comandos que se utiliza para implementar un sistema operativo en el sistema administrado mediante SCCM.

Antes de crear una Plantilla operativa, Dell EMC recomienda completar los siguientes requisitos previos.

- En Configuration Manager, asegúrese de que el sistema esté descubierto y que aparezca en **Activos y cumplimiento > Colecciones de dispositivos > Todos los servidores Dell Lifecycle Controller**. Para obtener más información, consulte [Descubrir 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.

Tipos de secuencia de tareas

Puede crear una secuencia de tareas de dos maneras:

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

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

Crear una secuencia de tareas específica de Dell

Para crear una secuencia de tareas específica de Dell utilizando la opción **Plantilla de implementación de servidores OMIMSSC** en SCCM:

1. Inicie Configuration Manager.
Aparece 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 secundario en **Secuencias de tareas** y, luego, en **Implementación de servidor OMIMSSC > Crear una plantilla de implementación de servidores OMIMSSC**.
Aparece el **Asistente de secuencias de tareas de implementación de servidor OMIMSSC**.
4. Escriba el nombre de la secuencia de tareas en el campo **Nombre de 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 **Instalación del sistema operativo**, seleccione el tipo de instalación del sistema operativo. Las opciones son:
 - **Usar una imagen WIM del sistema operativo**
 - **Instalación del sistema operativo mediante una secuencia de comandos**
7. Seleccione un paquete del sistema operativo en el menú desplegable **Paquete del sistema operativo por usar**.
8. Si tiene un paquete con **unattend.xml**, entonces selecciónelo desde el menú **Paquete con información de archivo unattend.xml**, o bien seleccione **<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

NOTA: Durante la edición de una secuencia de tareas en SCCM 2016 y 2019, los mensajes de referencia de objetos faltantes no muestran el paquete **Setup windows and ConfigMgr**. Agregue el paquete y, luego, guarde la secuencia de tareas.

1. Inicie Configuration Manager.
Aparece la pantalla de Configuration Manager.
2. En el panel izquierdo, seleccione **Biblioteca de software > Sistemas operativos > Secuencias 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 desde Dell Lifecycle Controller**.
Se carga la acción personalizada para la implementación del servidor Dell. Ahora puede realizar cambios en la secuencia de tareas.

NOTA: Cuando edita una secuencia de tareas por primera vez, se muestra el mensaje de error **Configuración de Windows y Configuration Manager**. Para resolver el error, cree y seleccione el paquete de actualización del cliente de Configuration Manager. Para obtener más información sobre la creación de paquetes, consulte la documentación de Configuration Manager en technet.microsoft.com.

NOTA: Durante la edición de una secuencia de tareas en SCCM 2016 y 2019, los mensajes de referencia de objetos faltantes no muestran el paquete Setup windows and ConfigMgr. Por ende, debe agregar el paquete y, luego, guardar la secuencia de tareas.

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

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

1. En **Configuration Manager**, seleccione **Administración > Configuración de sitio > Sitios**
2. Haga clic con el botón secundario en **<nombre del servidor de sitio>**, seleccione **Configurar componentes de sitio y**, luego, **Administración fuera de banda**.
Aparecerá la ventana **Propiedades de los componentes de administración fuera de banda**.
3. Haga clic en la pestaña **Lifecycle Controller**.
4. 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.
5. En la ventana **Modificar información de recurso compartido**, introduzca un nuevo nombre de recurso compartido y una ruta nueva de acceso al recurso compartido.
6. Haga clic en **Aceptar**.

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

1. En Configuration Manager, en la sección **Biblioteca de software**, haga clic con el botón secundario en **Secuencias de tareas** y seleccione **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.
 - NOTA:** OMIMSSC no admite el método de medios independientes para crear medios de secuencias de tareas.
2. Desde el **Asistente de medios de secuencia de tareas**, seleccione **Medios de arranque**, seleccione **Permitir implementación desatendida del sistema operativo** y haga clic en **Siguiente**.
3. Seleccione **Conjunto de CD/DVD**, haga clic en **Examinar** y seleccione la ubicación para guardar la imagen ISO.
4. Haga clic en **Siguiente**.
5. Desactive la casilla de verificación **Proteger medio con una contraseña** y haga clic en **Siguiente**.
6. Desplácese y seleccione **Imagen de arranque de implementación de servidor PowerEdge**.
 - NOTA:** Utilice la imagen de arranque creada utilizando solo DTK.
7. Seleccione el punto de distribución del menú desplegable y luego seleccione la casilla de verificación **Mostrar puntos de distribución de los sitios secundarios**.
8. Haga clic en **Siguiente**.
Aparece la pantalla **Resumen** con la información del medio de secuencia de tareas.
9. Haga clic en **Siguiente**.
Se muestra la barra de progreso.
10. Cuando finalice la creación de la imagen, cierre el asistente.

Preparación para implementar un sistema operativo distinto a Windows

Asegúrese de recordar los siguientes puntos para implementar sistemas operativos distintos a Windows en sistemas administrados:

- El archivo ISO está disponible en una versión NFS (Sistema de archivos de red) o una versión de recurso compartido CIFS (Sistema de archivos de Internet común) con acceso de lectura y escritura.
- Confirme que la unidad virtual está disponible en el sistema administrado.
- Después de implementar el sistema operativo ESXi, el servidor se mueve a la recopilación de **Lifecycle Controller administrado (ESXi)** en SCCM.
- Después de implementar cualquier tipo de sistema operativo distinto a Windows, los servidores se mueven al **grupo de actualización predeterminado de host distinto a Windows**.
- Se recomienda que el adaptador de red esté conectado al puerto de la red del servidor en el que se instala el sistema operativo.

Crear clústeres utilizando una Plantilla operativa

En este capítulo, se incluye información acerca de cómo crear los clústeres de Storage Spaces Direct.

Temas:

- [Crear un switch lógico para clústeres de Storage Spaces Direct](#)
- [Creación de clústeres de Storage Spaces Direct](#)

Crear un switch lógico para clústeres de Storage Spaces Direct

Cree un switch lógico desde OMIMSSC en SCVMM.

NOTA: La dirección IP que se ingresa en la sección **Configuración para la administración** anula la dirección IP que se ingresó en el componente del sistema operativo de la Plantilla operativa predefinida para Storage Spaces Direct.

1. En OMIMSSC, expanda **Configuración e implementación**, haga clic en **Vista de clúster** y, luego, haga clic en **Crear switch lógico para clúster**.
2. Proporcione un nombre para el switch lógico y seleccione el grupo de host presente en SCVMM para asociar el switch lógico.
3. Ingrese los siguientes detalles y haga clic en **Crear**.
 - a. En **Configuración para la administración**, proporcione los datos de **subred**, **IP de inicio**, **IP de fin**, **servidor DNS**, **sufijo DNS** y **puerta de enlace**.

NOTA: Proporcione la información de subred en la notación CIDR (enrutamiento de interdominios sin clases).
 - b. En **Configuración de almacenamiento**, proporcione los datos de **VLAN**, **subred**, **IP de inicio** e **IP de fin**.
4. Ingrese un nombre único de trabajo y una descripción para el trabajo; luego, haga clic en **Crear**.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Para verificar que el switch lógico se creó correctamente, compruebe si el nombre del switch lógico aparece en el menú desplegable de la página **Crear clúster**.

Para ver los detalles del switch lógico, realice los siguientes pasos en SCVMM:

1. Para ver el nombre del switch lógico, haga clic en **Fabric** y, en la sección **Redes**, haga clic en **Switches lógicos**.
2. Para ver el perfil de puerto de enlace ascendente (UPP) del switch lógico, haga clic en **Fabric** y, en la sección **Redes**, haga clic en **Switches lógicos**.
3. Para ver la red del switch lógico, haga clic en **Fabric** y, en la sección **Redes**, haga clic en **Redes lógicas**.

Creación de clústeres de Storage Spaces Direct

- Asegúrese de crear una red lógica mediante la función **Configurar switch lógico para el clúster**.
- Asegúrese de utilizar SCVMM 2016 o 2019.
- Asegúrese de utilizar Windows Server 2016 o 2019 Datacenter Edition.
- Asegúrese de que las configuraciones de los servidores administrados tengan el mismo firmware que la solución Storage Spaces Direct y que cumplan con los requisitos de las versiones de controlador. Para obtener más información, consulte la documentación *Matriz de soporte para nodos Dell EMC Storage Spaces Direct Ready PowerEdge R740XD, R740XD2 y PowerEdge R640*.

- Para obtener información sobre administración e infraestructura de Storage Spaces Direct, consulte la documentación *Guía de implementación de nodos Dell EMC Microsoft Storage Spaces Direct Ready para infraestructura hiperconvergente escalable con nodos Storage Spaces Direct Ready R740xd, R740XD2 y R640*.

NOTA: Storage Spaces Direct (S2D) también se conoce como Windows Server definido por software (WSSD) e infraestructura hiperconvergente Azure Stack (ASHCI).

Tenga en cuenta lo siguiente antes de crear clústeres de Storage Spaces Direct:

- Puede crear un clúster de Storage Spaces Direct en OMIMSSC ingresando solo una dirección IP estática.
- El tamaño del disco virtual se muestra como cero en la plantilla operativa predefinida de Storage Spaces Direct. Sin embargo, después de aplicar la plantilla operativa predefinida de Storage Spaces Direct, la unidad virtual se crea solo con un tamaño igual al tamaño completo del medio de almacenamiento físico M.2. Para obtener más información acerca del espacio de unidad virtual, consulte la Guía del usuario de iDRAC disponible en dell.com/support.
- Debe asegurarse de que la dirección IP esté configurada en la plantilla operativa, si la opción de paso de sistema operativo a iDRAC está habilitada.

Para crear un clúster de Storage Spaces Direct, realice los siguientes pasos:

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de clúster**. Aparece la página **Vista de clúster**.
2. Ingrese un nombre de clúster y seleccione la Plantilla operativa predefinida para crear clústeres de Storage Spaces Direct.
 - Los servidores sin asignar que pertenecen solo a un modelo de servidor y una tarjeta NIC en específico aparecen según la Plantilla operativa que seleccionó en el menú desplegable **Plantilla operativa**.
3. Para agregar servidores a un clúster, seleccione los servidores utilizando la casilla de verificación.
4. Para agregar los valores de pool específicos de un sistema, haga clic en **Exportar pool de valor de atributo**. Edite y guarde el archivo para que pueda proporcionar los valores de pool específicos de un sistema. Para obtener más información, consulte [Completar el archivo CSV de valor de pool](#).
5. (Opcional) Si debe establecer valores específicos de un sistema, vaya a **Pool de valor de atributo**, haga clic en **Examinar** y seleccione el archivo .CSV editado.
6. Ingrese un nombre de trabajo único y haga clic en **Crear**.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

NOTA: Cuando la implementación del sistema operativo está en curso, verá que se están clonando perfiles de computadora física o un perfil de host en SCVMM (nombre anexado con GUID del servidor). Estos perfiles se consumen para fines de visualización en pantalla (OSD) de un servidor individual.

Para comprobar si los clústeres se crearon correctamente:

1. Verifique que el trabajo de creación de clúster muestre el estado "Realizado con éxito".
2. Vea el clúster en la página **Vista de clúster**.
3. Vea el clúster en SCVMM.

Para obtener más información, consulte la sección [Crear un perfil de equipo físico](#) en la sección Requisitos previos de la documentación de Microsoft sobre el aprovisionamiento de un host o clúster de Hyper-V desde computadoras vacías.

NOTA: Se recomienda configurar el testigo de clúster para un clúster de dos nodos. La configuración del testigo de clúster ayuda a mantener un clúster o un cuórum de almacenamiento cuando falla un nodo o una comunicación de red. Para obtener más información, consulte la [Guía de implementación de Storage Spaces Direct](#).

Actualización del firmware en OMIMSSC

Mantenga actualizados los dispositivos Dell EMC actualizando al firmware más reciente mediante OMIMSSC para utilizar funciones de seguridad, correcciones de problemas y otras mejoras. Actualice el firmware de los dispositivos mediante los repositorios de actualización de Dell EMC.

Actualizar el firmware solo se permite en dispositivos compatibles de hardware. Para utilizar las funciones disponibles en OMIMSSC en los dispositivos administrados, estos dispositivos deben tener las versiones de firmware mínimas requeridas de iDRAC, Lifecycle Controller (LC) y el BIOS. Los dispositivos que tengan las versiones de firmware necesarias son equipos compatibles de hardware.

Temas:

- [Acerca de los grupos de actualización](#)
- [Acerca de los orígenes de actualización](#)
- [Integración en Dell EMC Repository Manager \(DRM\)](#)
- [Establecer la frecuencia de sondeo](#)
- [Visualización y actualización del inventario de dispositivos](#)
- [Aplicar filtros](#)
- [Actualizar y revertir versiones de firmware mediante el método Ejecutar actualización](#)

Acerca de los grupos de actualización

Los grupos de actualización son un grupo de dispositivos que requieren una administración de actualizaciones similar. Existen dos tipos de grupos de actualización compatibles en OMIMSSC:

- Grupos de actualización predefinidos: no puede crear, modificar ni eliminar manualmente los grupos de actualización predefinidos.
- Grupos de actualización personalizados: puede crear, modificar y eliminar dispositivos en estos grupos.

NOTA: Todos los grupos de servidores que existen en SCVMM aparecen en OMIMSSC. Sin embargo, la lista de servidores en OMIMSSC no es específica de algún usuario. Por lo tanto, asegúrese de contar con acceso para realizar cualquier operación en dichos dispositivos.

Grupos de actualización predefinidos

Después de detectar un dispositivo, el dispositivo descubierto se agrega a uno de los siguientes grupos predefinidos.

- **Grupos de hosts predeterminados:** este grupo se compone de servidores implementados en un sistema operativo Windows o sincronizados con una consola Microsoft registrada.
- **Grupos predeterminados sin asignar:** este grupo se compone de servidores descubiertos sin asignar o de bajo nivel.
- **Grupos de hosts predeterminados que no son de Windows:** este grupo se compone de servidores implementados en sistemas operativos distintos a Windows.
- **Grupos de actualización de chasis:** este grupo se compone de servidores, chasis o sistemas modulares. El descubrimiento de servidores de 12.^a generación en adelante incluye su información de chasis. De manera predeterminada, se crea un grupo con el siguiente formato de nombre: `Chassis-Service-tag-of-Chassis-Group` (Etiqueta de servicio del chasis del grupo de chasis). Por ejemplo: `Chassis-GJDC4BS-Group`. Si se elimina un servidor modular de un grupo de actualización de clúster, entonces se agrega el servidor al grupo de actualización de chasis junto con su información de CMC. Incluso si no existen servidores modulares en el grupo de actualización de chasis correspondiente, debido a que todos los servidores modulares en el chasis se encuentran en un grupo de actualización de clúster, el grupo de actualización de chasis sigue existiendo, pero solo muestra la información de CMC.
- **Grupos de actualización de clúster:** este grupo se compone de **clústeres de conmutación por error de Windows Server**. Si un servidor modular de 12.^a generación en adelante es parte de un clúster, entonces también se agrega la información de CMC en el inventario de la página **Centro de mantenimiento**.

Grupos de actualización personalizado

Para crear grupos de actualización personalizados de tipo **Grupo de actualización genérico**, agregue los dispositivos descubiertos en grupos que requieran una administración similar. Sin embargo, solo puede agregar un dispositivo a un grupo de actualización personalizado desde **grupos de actualización predeterminados sin asignar** y **grupos de actualización de host predeterminados**. Para agregar los servidores a un grupo de actualización personalizado, busque el dispositivo requerido mediante su etiqueta de servicio. Después de agregar un dispositivo a un grupo de actualización personalizado, se elimina el dispositivo del grupo de actualización predefinido y solo estará disponible en el grupo de actualización personalizado.

Visualización grupos de actualización

Para ver grupos de actualización:

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento** y, luego, en **Configuración de mantenimiento**.
2. En **Configuración de mantenimiento**, haga clic en **Actualizar grupos**.
Se muestran todos los grupos personalizados creados con el nombre, el tipo de grupo y el número de servidores en el grupo.

Creación de grupos actualización personalizados

1. En la consola de OMIMSSC, haga clic en **Centro de mantenimiento** y, luego, en **Configuración de mantenimiento**.
2. En **Configuración de mantenimiento**, haga clic en **Grupos de actualización** y, a continuación, haga clic en **Crear**. Aparece la página **Grupo de actualización del firmware**.
3. Ingrese un nombre de grupo y una descripción, y seleccione el tipo de grupo de actualización que desea crear.
Los grupos de actualización personalizados solo pueden tener servidores de los siguientes tipos de grupos de actualización:
 - Grupo de actualización genérico: se compone de servidores de grupos de actualización sin asignar predeterminados y de grupos de actualización de host predeterminados.
 - Grupo de actualización de host: se compone de servidores de grupos de actualización de host predeterminados.También puede tener una combinación de servidores con los dos tipos de grupos de servidores.
4. Para agregar servidores al grupo de actualización, busque los servidores mediante su etiqueta de servicio y, para agregar servidores a la tabla **Servidores incluidos en el grupo de actualización**, haga clic en la flecha derecha.
5. Para crear el grupo de actualización personalizado, haga clic en **Guardar**.
Nota: El grupo de actualización personalizado es específico del centro de sistemas y será visible para otros usuarios del mismo centro de sistemas.

Modificación de grupos actualización personalizados

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 mover servidores de un grupo de actualización personalizado a otro grupo de actualización personalizado, puede hacerlo de la siguiente forma:
 1. Elimine el servidor de un grupo de actualización personalizado existente. Así se agrega automáticamente en el grupo de actualización predefinido.
 2. Edite el grupo personalizado para agregar el servidor y, a continuación, busque el servidor mediante la etiqueta de servicio.
1. En **OMIMSSC**, haga clic en **Centro de mantenimiento** y, luego, en **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

Tenga en cuenta los siguientes puntos cuando elimine un grupo de actualización personalizado en las siguientes circunstancias:

- No puede eliminar un grupo de actualización si tiene un trabajo programado, en curso o a la espera. Por lo tanto, elimine los trabajos programados que están asociados con un grupo de actualización personalizado antes de eliminar el grupo de servidores.

- Puede eliminar un grupo de actualización, incluso si los servidores están presentes en dicho grupo de actualización. Sin embargo, después de eliminar ese grupo de actualización, los servidores se mueven a sus respectivos grupos de actualización predefinidos.
 - Si un dispositivo presente en un grupo de actualización personalizado se elimina de la MSSC y ejecuta una sincronización OMIMSSC con la MSSC inscrita, el dispositivo se elimina del grupo de actualización personalizado y se mueve al grupo predefinido correspondiente.
1. En **OMIMSSC**, haga clic en **Centro de mantenimiento** y, luego, en **Configuración de mantenimiento**.
 2. En **Configuración de mantenimiento**, haga clic en **Grupos de actualización**, seleccione el grupo de actualización, y, a continuación, haga clic en **Eliminar** para eliminar el grupo de actualización.

Acerca de los orígenes de actualización

Los orígenes de actualización hacen referencia a los archivos de catálogo que contienen actualizaciones de Dell EMC (BIOS, paquetes de controladores como componentes de administración, tarjetas de red) e incluyen los archivos ejecutables autocontenidos denominados Dell Update Packages (DUP).

Puede crear un origen de actualización o un repositorio, y configurarlo como un origen de actualización predeterminado para generar un informe de comparación y recibir alertas cuando haya nuevos archivos de catálogo disponibles en el repositorio.

Mediante OMIMSSC, puede mantener actualizado el firmware de los dispositivos utilizando orígenes de actualización en línea u offline.

Los orígenes de actualización en línea son repositorios mantenidos gracias a Dell EMC.

Los orígenes de actualización offline son repositorios locales que se utilizan cuando no hay conexión a Internet.

Se recomienda crear repositorios personalizados y colocar el recurso compartido de red en la intranet local del dispositivo de OMIMSSC. Esto permite reducir el consumo del ancho de banda de Internet y también proporciona un repositorio interno seguro.

Actualice el firmware mediante uno de los siguientes orígenes de actualización:

- **Repositorio DRM:** es un repositorio offline. Exporte la información de inventario de los dispositivos descubiertos desde el dispositivo de OMIMSSC para preparar un repositorio en DRM. Para obtener más información acerca de la integración en DRM y la creación de un origen de actualización mediante DRM, consulte [Integración en DRM](#). Después de crear un repositorio en DRM, vaya a OMIMSSC y seleccione el origen de actualización creado mediante DRM y los dispositivos correspondientes, e inicie una actualización en los dispositivos. Para obtener más información acerca de DRM, consulte los documentos sobre *Dell Repository Manager* disponibles en `dell.com\support`.
 - **FTP, HTTP o HTTPS:** pueden ser un repositorio en línea o sin conexión. Actualice los componentes específicos de dispositivos con la actualización más reciente proporcionada en el sitio FTP, HTTP o HTTPS. Mediante Dell EMC, se prepara un repositorio que vence cada dos meses y se publican las siguientes actualizaciones a través de catálogos PDK:
 - BIOS y firmware del servidor
 - Paquetes del controlador del sistema operativo certificados por Dell EMC: para la implementación del sistema operativo
- NOTA:** Si selecciona un origen de actualización en línea mientras implementa la Plantilla operativa, las versiones de firmware más recientes se descargan y aplican en los dispositivos administrados. Por lo tanto, las versiones de firmware pueden variar entre el dispositivo de referencia y el dispositivo implementado.
- **Inventario de firmware de referencia y comparación:** se puede convertir en un repositorio offline mediante DRM. Cree un archivo de inventario de referencia que contenga el inventario de firmware de los dispositivos seleccionados. El archivo de inventario de referencia puede contener información de inventario de un dispositivo del mismo tipo o modelo, o bien puede tener varios dispositivos de diferentes tipos o modelos. Puede comparar la información de inventario de los dispositivos presentes en OMIMSSC con el archivo de inventario de referencia guardado. Para mover el archivo exportado a DRM y crear un repositorio, consulte los documentos sobre *Dell Repository Manager* disponibles en `dell.com\support`.

Origen de actualización predefinido y predeterminado

OMIMSSC incluye tres orígenes de actualización predefinidos que están disponibles después de una nueva instalación o actualización. El **CATÁLOGO FTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo FTP, el **CATÁLOGO HTTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo HTTP y el **CATÁLOGO HTTPS EN LÍNEA DE DELL** es un origen de actualización predeterminado de tipo HTTPS. Sin embargo, puede crear otro origen de actualización y marcarlo como un origen de actualización predeterminado.

NOTA: Si utiliza un servidor proxy, para acceder al repositorio, debe editar el origen de actualización para agregar los detalles de proxy y guardar los cambios.

Orígenes de actualización predefinidos y predeterminados para clústeres de Storage Spaces Direct

OMIMSSC admite la actualización de clústeres de Storage Spaces Direct mediante orígenes de actualización predefinidos en específico. Estos orígenes de actualización hacen referencia a archivos de catálogo que contienen las versiones recomendadas de firmware más recientes de los componentes para clústeres de Storage Spaces Direct. Solo aparecen en la página **Centro de mantenimiento**.

El **CATÁLOGO S2D FTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo FTP que forma parte del **CATÁLOGO FTP EN LÍNEA DE DELL**.

El **CATÁLOGO S2D HTTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo HTTP que forma parte del **CATÁLOGO HTTP EN LÍNEA DE DELL**.

El **CATÁLOGO HTTPS EN LÍNEA S2D DE DELL** es un origen de actualización predeterminado de tipo HTTPS que forma parte del **CATÁLOGO HTTPS EN LÍNEA DE DELL**.

NOTA: Storage Spaces Direct (S2D) también se conoce como Windows Server definido por software (WSSD) e infraestructura hiperconvergente Azure Stack (ASHCI).

Orígenes de actualización predefinidos y predeterminados para sistemas modulares

OMIMSSC admite la actualización de sistemas modulares mediante orígenes de actualización predefinidos en específico. Estos orígenes de actualización hacen referencia a archivos de catálogo que contienen las versiones recomendadas de firmware más recientes de los componentes para sistemas modulares. Solo aparecen en la página **Centro de mantenimiento**.

El **CATÁLOGO MX7000 FTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo FTP que forma parte del **CATÁLOGO FTP EN LÍNEA DE DELL**.

El **CATÁLOGO MX7000 HTTP EN LÍNEA DE DELL** es un origen de actualización predefinido de tipo HTTP que forma parte del **CATÁLOGO HTTP EN LÍNEA DE DELL**.

El **CATÁLOGO MX7000 HTTPS EN LÍNEA DE DELL** es un origen de actualización predeterminado de tipo HTTPS que forma parte del **CATÁLOGO HTTPS EN LÍNEA DE DELL**.

Validar datos mediante una conexión de prueba

Utilice **Conexión de prueba** para verificar si se puede acceder a la ubicación del origen de actualización mediante las credenciales mencionadas durante la creación del origen de actualización. Solo podrá crear un origen de actualización después de que la conexión se realice correctamente.

Configuración de FTP local

Para configurar un 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.gz` desde el FTP en línea y descomprima 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 la ubicación base **baseLocation** 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

Para configurar un 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.gz` desde el 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 la ubicación base **baseLocation** a la URL del HTTP local y, luego, comprima el archivo con la extensión `.gz`.
Por ejemplo, cambie el **baseLocation** de `downloads.dell.com` al nombre de host o la dirección IP como `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`.

Configuración de HTTPS local

Para configurar un HTTPS local:

1. Cree una estructura de carpetas en el HTTPS local que sea una réplica exacta de `downloads.dell.com`.
2. Descargue el archivo `catalog.gz` desde el HTTPS en línea en la siguiente ubicación: `https://downloads.dell.com/catalog/catalog.xml.gz` y extraiga los archivos.
3. Extraiga el archivo `catalog.xml`, cambie la **baseLocation** a la URL del HTTPS local y luego comprima el archivo con la extensión `.gz`.
Por ejemplo, cambie el **baseLocation** de `downloads.dell.com` al nombre de host o la dirección IP como `hostname.com`.
4. Coloque el archivo de catálogo con el archivo de catálogo modificado y los archivos DUP en su carpeta HTTPS local replicando la misma estructura de `downloads.dell.com`.

Visualización del origen de actualizaciones

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento**.
2. En **Centro de mantenimiento**, haga clic en **Configuración de mantenimiento** y, a continuación, haga clic en **Origen de actualización**.
Se muestran todos los orígenes de actualización creados junto con su descripción, tipo de origen, ubicación y nombre perfil de credencial.

Creación de un origen de actualizaciones

- Según el tipo de origen de actualización, asegúrese de que haya disponible un perfil de credenciales de Windows o FTP.
 - Si crea un origen de actualización de DRM, asegúrese de instalar y configurar DRM utilizando funciones de administrador.
1. En **OMIMSSC**, haga clic en **Centro de mantenimiento** y, luego, en **Configuración de mantenimiento**.
 2. En la página **Origen de actualización**, haga clic en **Crear nueva** e ingrese el nombre y la descripción del origen de actualización.
 3. Seleccione uno de los siguientes tipos de origen de actualización desde el menú desplegable **Tipo de origen**:
 - Orígenes FTP: seleccione esta opción para crear un origen de actualización FTP local o en línea.
i **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.
 - Orígenes HTTP: seleccione esta opción para crear un origen de actualización HTTP local o en línea.
i **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.
 - Orígenes HTTPS: seleccione esta opción para crear un origen de actualización HTTPS en línea.
i **NOTA:** Si va a crear un origen de actualización de tipo HTTPS, proporcione la ruta de acceso completa del catálogo con el nombre de catálogo y sus credenciales de proxy para acceder al origen de actualización.

Repositorio DRM: seleccione esta opción para crear un origen de actualización de repositorio local. Asegúrese de que DRM esté instalado.

NOTA: Si va a crear una fuente DRM, ingrese sus credenciales de Windows y asegúrese de que se pueda acceder a la ubicación compartida de Windows. En el campo Ubicación, ingrese la ruta completa del archivo de catálogo con el nombre de archivo.

- Archivos de salida de inventario: seleccione esta opción para ver el inventario de firmware en contraste con la configuración del servidor de referencia.

NOTA: Puede ver un informe de comparación utilizando los **archivos de salida de inventario** como origen de actualización. La información de inventario del servidor de referencia se compara con todos los otros servidores descubiertos en OMIMSSC.

- En **Ubicación**, ingrese la URL del origen de actualización de un origen FTP, HTTP o HTTPS y la ubicación compartida en Windows para DRM.

NOTA: El sitio FTP local debe replicar al FTP en línea.

NOTA: El sitio HTTP local debe replicar al HTTP en línea.

NOTA: No es obligatorio ingresar HTTP o HTTPS en la URL para una fuente FTP.

- Para acceder al origen de actualización, seleccione el perfil de credencial necesario en **Credenciales**.
- En **Credenciales de proxy**, seleccione las credenciales de proxy correspondientes si es necesario un proxy para acceder a la fuente FTP o HTTP.
- (Opcional) Para que el origen de actualización creada sea el origen predeterminado, seleccione **Convertir en origen predeterminado**.
- Para verificar que se pueda acceder a la ubicación del origen de actualización mediante las credenciales mencionadas, haga clic en **Probar conexión** y, luego, en **Guardar**.

NOTA: Solo puede crear el origen de actualización después de que la prueba de conexión finalice correctamente.

Modificación del origen de actualizaciones

Tenga en cuenta los siguientes puntos antes de modificar un origen de actualización:

- Para editar el origen de actualización de **CATÁLOGO S2D FTP EN LÍNEA DE DELL**, **CATÁLOGO S2D HTTP EN LÍNEA DE DELL** o **CATÁLOGO S2D HTTPS EN LÍNEA DE DELL**, edite el origen de actualización predefinido correspondiente y guarde los cambios. Esta actualización se refleja en el origen de actualización del **CATÁLOGO S2D FTP EN LÍNEA DE DELL**, **CATÁLOGO S2D HTTP EN LÍNEA DE DELL** o **CATÁLOGO S2D HTTPS EN LÍNEA DE DELL**.
- 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 **Confirmar** para ir a los cambios.
- Cuando se actualiza un archivo de catálogo en el origen de actualización, el archivo de catálogo en caché local no se actualiza automáticamente. Para actualizar el archivo de catálogo guardado en caché, edite el origen de actualización o elimine y vuelva a crear el origen de actualización.

Seleccione el origen de actualización que desea modificar, haga clic en **Editar** y, luego, actualice el origen según sea necesario.

Eliminación de origen de actualizaciones

Tenga en cuenta los siguientes puntos antes de eliminar un origen de actualización:

- No puede eliminar un origen de actualización predefinido.
- No puede eliminar un origen de actualización si se utiliza en un trabajo en curso o un trabajo programado.
- No puede eliminar un origen de actualización si es un origen predeterminado.

Seleccione el origen de actualización que desea eliminar y haga clic en **Eliminar**.

Integración en Dell EMC Repository Manager (DRM)

OMIMSSC OMIMSSC está integrado en DRM para crear fuentes de actualización personalizadas en OMIMSSC. La integración está disponible desde DRM versión 2.2 en adelante. Proporcione la información del dispositivo detectado desde el dispositivo OMIMSSC a DRM; utilizando la información de inventario disponible, puede crear un repositorio personalizado en DRM y establecerlo como una fuente de actualización en OMIMSSC para realizar actualizaciones de firmware y crear clústeres en dispositivos administrados. Para obtener más información acerca de la creación de un repositorio en DRM, consulte los documentos sobre *Dell EMC Repository Manager* disponibles en dell.com/support/home.

Integración de DRM con OMIMSSC OMIMSSC

En esta sección, se describe el proceso para crear un repositorio con integración.

- i** **NOTA:** Tenga en cuenta varios factores como el ambiente de pruebas, las actualizaciones de seguridad, las recomendaciones de aplicación y las asesorías de Dell EMC para preparar las actualizaciones necesarias.
 - i** **NOTA:** Para ver la información de inventario más reciente acerca de los dispositivos detectados, después de actualizar OMIMSSC, reintegre DRM con el dispositivo OMIMSSC.
1. En la página de inicio, haga clic en **Agregar nuevo repositorio**. Aparece la ventana **Agregar repositorio nuevo**.
 2. Seleccione la pestaña **Integración**, ingrese el **nombre del repositorio** y una **descripción**.
 3. Seleccione **Personalizado** y haga clic en **Elegir sistemas** para seleccionar cualquier sistema específico.
 4. En el menú desplegable **Tipo de integración**, seleccione el producto con el cual desea realizar una integración. Según el producto seleccionado, se muestran las siguientes opciones. Las opciones disponibles son:
 - a. Integración de Dell OpenManage para Microsoft System Center: proporcione el nombre de host o la dirección IP, el nombre de usuario, la contraseña y el servidor proxy.
 - i** **NOTA:** Asegúrese de que la contraseña no contenga caracteres especiales, como <, >, ', ", &.
 - b. Integración de consola de Dell: proporcione la URL <https://<IP>/genericconsolerepository>, el nombre de usuario del administrador, la contraseña y el servidor proxy.
 - i** **NOTA:** La integración de la consola de Dell se aplica para las consolas que incorporan los servicios web, como OpenManage Integration para System Center Virtual Machine Manager (SCVMM).
 5. Después de seleccionar la opción necesaria, haga clic en **Conectar**. El sistema y el modelo disponibles se mostrarán en la sección **Tipo de integración**.
 6. Seleccione **Agregar** para crear el repositorio. El repositorio se muestra en el tablero del repositorio que está disponible en la página de inicio.

Nota: Durante la selección de los tipos de paquetes o los formatos DUP, asegúrese de seleccionar Windows de 64 bits y el sistema operativo de manera independiente, en caso de que el chasis Dell PowerEdge MX7000 sea parte del inventario en OMIMSSC.

Después de integrar DRM en OMIMSSC, consulte la sección *Obtener el catálogo de firmware para nodos Storage Spaces Direct Ready mediante Dell Repository Manager* de la *Guía de operaciones de nodos Dell EMC Microsoft Storage Spaces Direct Ready para administrar y supervisar el ciclo de vida de un nodo Ready* en dell.com/support dell.com/support

Establecer la frecuencia de sondeo

Configure el sondeo y las notificaciones para recibir alertas cuando hay un nuevo archivo de catálogo disponible en el origen de actualización; estas opciones están seleccionadas de forma predeterminada. El dispositivo de OMIMSSC guarda una caché local del origen de actualización. El color de la campana de notificación cambia a color naranja cuando hay un nuevo archivo de catálogo disponible en el origen de actualización. Para reemplazar el catálogo almacenado en caché local que está disponible en el dispositivo de OMIMSSC, haga clic en el ícono de campana. Después de reemplazar el archivo de catálogo antiguo con el archivo de catálogo más reciente, la campana cambia a color verde.

Para configurar la frecuencia de sondeo:

1. En OMIMSSC, haga clic en **Centro de mantenimiento** y, luego, en **Sondeo y notificación**.
2. Seleccione la frecuencia en la que se llevará a cabo el sondeo:

- **Nunca:** esta opción está seleccionada de manera predeterminada. Seleccione esta opción para no recibir actualizaciones nunca.
- **Una vez a la semana:** seleccione esta opción para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualización de forma semanal.
- **Una vez cada 2 semanas:** seleccione esta opción para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualización una vez cada dos semanas.
- **Una vez al mes:** seleccione esta opción para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualización mensualmente.

Visualización y actualización del inventario de dispositivos

Vea un informe de comparación para los dispositivos en contraste con un origen de actualización en la página **Centro de mantenimiento**. Cuando selecciona un origen de actualización, aparece un informe que compara el firmware existente con el firmware presente en el origen de actualización seleccionada. El informe se genera dinámicamente cuando cambia de origen de actualización. Se compara el inventario del servidor con el origen de actualización y se muestran las acciones sugeridas. Esta actividad demora un tiempo considerable dependiendo de la cantidad de dispositivos y de los componentes de dispositivo presentes. No puede realizar otras tareas durante este proceso. La actualización de inventario actualiza todo el inventario del dispositivo, incluso aunque seleccione un único componente en ese dispositivo.

A veces, se actualiza el inventario del dispositivo, pero la página no muestra el inventario más reciente. Por lo tanto, utilice la opción Actualizar para ver la información más reciente del inventario de los dispositivos descubiertos.

NOTA: Después de actualizar a la versión más reciente de OMIMSSC, si falla la conexión con `ftp.dell.com` o `downloads.dell.com`, la fuente de actualización de FTP, HTTP o HTTPS en línea predeterminada de Dell no puede descargar el archivo del catálogo. Por lo tanto, el informe de comparación no estará disponible. Para ver un informe de comparación para el origen de actualización predeterminado, edite el FTP en línea predeterminado de Dell, el origen de actualización HTTP de Dell o HTTPS de Dell (proporcione las credenciales de proxy si es necesario) y, luego, seleccione lo mismo desde el menú desplegable **Seleccionar origen de actualización**. Para obtener más información acerca de cómo editar un origen de actualización, consulte [Modificar un origen de actualización](#).

NOTA: Cuando entregue el producto, encontrará una copia local del archivo del catálogo en OMIMSSC. Por lo tanto, el informe de comparación más reciente no estará disponible. Para ver el último informe de comparación, actualice el archivo de catálogo. Para actualizar el archivo de catálogo, edite el origen de actualización y guárdela, o bien elimínela y vuelva a crear un origen de actualización.

NOTA: En SCCM, incluso después de actualizar la información de inventario, los detalles de servidor como **Versión del paquete de controladores** y el sistema operativo de la opción **Controladores disponibles para** no se actualizan en la página de propiedades **Controladoras Dell fuera de banda (OOB)**. Para actualizar las propiedades de OOB, sincronice OMIMSSC con el SCCM inscrito.

NOTA: Cuando actualiza OMIMSSC, la información sobre los servidores detectados en versiones anteriores no aparece. Para obtener la última información del servidor y corregir el informe de comparación, vuelva a descubrir los servidores.

Para actualizar y visualizar el inventario de firmware de los dispositivos descubiertos:

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento**. Aparece la página **Centro de mantenimiento** con un informe de comparación para todos los dispositivos detectados en OMIMSSC en contraste con la fuente de actualización seleccionada.
2. (Opcional) Para ver un informe de comparación solo para un grupo específico de dispositivos, seleccione solo los dispositivos necesarios.
3. (Opcional) Para ver un informe de comparación para otro origen de actualización, cambie el origen de actualización seleccionando una desde la lista desplegable **Seleccionar origen de actualización**.
4. Para ver información de firmware de los componentes del dispositivo como la versión actual, la versión de línea base y las acciones de actualización recomendadas por Dell EMC, expanda el grupo de servidores desde **Grupo de dispositivos/servidores** a nivel de servidor y, luego, a nivel de componentes. También puede ver la cantidad de actualizaciones recomendadas para los dispositivos. Desplace el cursor sobre el ícono de actualizaciones disponibles para ver los detalles correspondientes de las actualizaciones, como la cantidad de actualizaciones críticas y las actualizaciones recomendadas.

El color indicador del ícono de actualizaciones disponibles se basa en la gravedad general de las actualizaciones; a continuación, se indican las categorías de actualización crítica:

- El color rojo fijo indica que hay una única actualización crítica en el servidor o grupo de servidores.
- El color amarillo indica que no hay actualizaciones críticas.
- El color verde indica que las versiones de firmware están actualizadas.

Después de llenar el informe de comparación, se sugieren las siguientes acciones de actualización:

- Degradar: existe una versión anterior disponible y puede cambiar la versión del firmware existente a esta versión.
- No se requieren acciones: el firmware existente es el mismo que el del origen de actualización.
- No hay actualizaciones disponibles: no hay actualizaciones disponibles para este componente.
 - ❗ **NOTA:** No hay actualizaciones disponibles para los componentes de unidad de fuente de alimentación (PSU) de los sistemas modulares y servidores MX7000 en los catálogos en línea. En caso de que desee actualizar el componente PSU para el sistema modular MX7000, consulte *Actualizar el componente de unidad de suministro de energía para dispositivos Dell EMC PowerEdge MX7000*. Para actualizar el componente PSU para servidores, póngase en contacto con el equipo de soporte de Dell EMC.
- Actualización (opcional): las actualizaciones son opcionales y consisten en nuevas características o actualizaciones de una configuración específica.
- Actualización (urgente): las actualizaciones son críticas y se utilizan para resolver situaciones críticas de seguridad, rendimiento o reparación de errores en componentes como BIOS.
- Actualización (recomendada): las actualizaciones son correcciones de problema o mejoras de función para los componentes. Además, se incluyen correcciones de compatibilidad con otras actualizaciones de firmware.

Aplicar filtros

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

Filtre el informe de comparación en función de los componentes de servidor disponibles. OMIMSSC admite tres categorías de filtros:

- **Tipo de actualización:** seleccione esta opción para filtrar y ver solamente el tipo seleccionado de actualizaciones en los servidores.
- **Tipo de componente:** seleccione esta opción para filtrar y ver solamente los componentes seleccionados en los servidores.
- **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 los filtros:

En OMIMSSC, haga clic en **Centro de mantenimiento**, haga clic en el menú desplegable de filtros y, luego, seleccione los filtros.

Eliminar filtros

Para quitar los filtros:

En OMIMSSC, haga clic en **Centro de mantenimiento** y, luego, haga clic en **Borrar filtros** o anule la selección de las casillas de verificación marcadas.

Actualizar y revertir versiones de firmware mediante el método Ejecutar actualización

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

- Hay un origen de actualización disponible.
 - ❗ **NOTA:** Seleccione una fuente de actualización de Storage Spaces Direct o fuentes de actualización de MX7000 para aplicar actualizaciones de firmware en clústeres de Storage Spaces Direct o en sistemas modulares de MX7000. Lo anterior se debe a que estas fuentes de actualización buscan una referencia modificada al catálogo que contenga versiones de firmware recomendadas de los componentes para clústeres Storage Spaces Direct y sistemas modulares.

- La cola de trabajos de iDRAC o del módulo Administración (MM) se borra antes de aplicar las actualizaciones en los dispositivos administrados.

Aplique actualizaciones en grupos de dispositivo seleccionados cuyo hardware sea compatible con OMIMSSC. Las actualizaciones se pueden aplicar inmediatamente, o bien pueden programarse. Los trabajos que se crean para actualizaciones de firmware aparecen en la página **Centro de trabajos y registros**.

Tenga en cuenta los siguientes puntos antes de actualizar o degradar el firmware:

- Cuando inicia esta tarea, esta demora un tiempo considerable dependiendo de la cantidad de dispositivos y de los componentes de dispositivo presentes.
 - Puede aplicar actualizaciones de firmware en un único componente de un dispositivo o a todo el entorno.
 - Si no existen actualizaciones ni degradaciones disponibles para un dispositivo, realizar una actualización de firmware en los dispositivos no provoca ninguna acción en los dispositivos.
 - Para actualizar el chasis, consulte la sección *Actualizar el firmware de CMC* en la *Guía del usuario del firmware de Dell PowerEdge M1000e Chassis Management Controller*.
 - Para actualizar el firmware del chasis en VRTX, consulte la sección *Actualizar el firmware* en la *Guía del usuario de Dell Chassis Management Controller para Dell PowerEdge VRTX*.
 - Para actualizar el firmware del chasis en FX2, consulte la sección *Actualizar el firmware* en la *Guía del usuario de Dell Chassis Management Controller para Dell PowerEdge FX2*.
1. En OMIMSSC, haga clic en **Centro de mantenimiento**, seleccione los servidores o grupos de sistema modular y una fuente de actualización; luego, haga clic en **Ejecutar actualización**.
 2. En **Detalles de la actualización**, proporcione el nombre y la descripción del trabajo de actualización de firmware.
 3. Para habilitar la degradación de las versiones de firmware, seleccione la casilla de verificación **Permitir degradación**. Si esta opción no está seleccionada, entonces no hay una acción en el componente que exija una degradación de firmware.
 4. En **Programar actualización**, seleccione una de las opciones siguientes:
 - **Ejecutar ahora**: seleccione para aplicar inmediatamente las actualizaciones.
 - Seleccione una fecha y hora para programar una actualización de firmware en el futuro.
 5. Seleccione alguno de los siguientes métodos y haga clic en **Completar**.
 - **Actualizaciones en etapas sin agente**: se aplican inmediatamente las actualizaciones que no requieren un reinicio de sistema y las actualizaciones que si requieren un reinicio se aplican cuando el sistema se reinicie. Para comprobar si se aplicaron todas las actualizaciones, actualice el inventario. Si la operación falla incluso en solo un dispositivo, todo el trabajo de actualización falla.
 - **Actualizaciones sin agente**: se aplican las actualizaciones y el sistema se reinicia inmediatamente.

NOTA: OMIMSSC solo admite **Actualizaciones sin agente** para los sistemas modulares MX7000.

NOTA: Actualización compatible con clústeres (CAU): automatiza el proceso de actualización mediante el uso de la función CAU de Windows en grupos de actualización de clúster para mantener la disponibilidad del servidor. Las actualizaciones pasan al coordinador de actualización de clúster presente en el mismo sistema en el cual está instalado el servidor SCVMM. El proceso de actualización es un proceso automatizado para mantener la disponibilidad del servidor. El trabajo de actualización se envía a la función Actualización compatible con clústeres (CAU) de Microsoft, sin importar la selección realizada desde el menú desplegable **Método de actualización**. Para obtener más información, consulte [Actualizar mediante CAU](#).

NOTA: Después de enviar un trabajo de actualización de firmware a iDRAC, OMIMSSC interactúa con iDRAC para solicitar el estado del trabajo y lo muestra en la página **Trabajos y registros** en el portal de administración de OMIMSSC. Si no hay respuesta desde iDRAC acerca del estado del trabajo por mucho tiempo, entonces el estado del trabajo se marca como fallido.

Integración en Dell EMC Repository Manager (DRM)

Las actualizaciones en servidores (que forman parte de un clúster) ocurren mediante el coordinador de actualización de clúster presente en el mismo sistema en el que se instala el servidor SCVMM. Las actualizaciones no ocurren por etapas y se aplican de inmediato. Mediante la actualización compatible con clústeres (CAU), puede minimizar cualquier interrupción o tiempo de inactividad de servidor, lo que permite una disponibilidad continua de la carga de trabajo. Por lo tanto, no afecta al servicio proporcionado por el grupo de clúster. Para obtener más información acerca de CAU, consulte la sección Descripción general de la actualización compatible con clústeres en technet.microsoft.com.

Antes de aplicar las actualizaciones en los grupos actualización de clúster, compruebe lo siguiente:

- Asegúrese de que el usuario registrado cuente con privilegios de administrador para actualizar clústeres mediante la función CAU.
- La conectividad con el origen de actualización seleccionado.
- La disponibilidad de los clústeres de conmutación por error.
- Verifique la preparación de la actualización del clúster y asegúrese de que no existan errores y avisos importantes en el informe "Preparación de clúster" para aplicar el método CAU. Para obtener más información acerca de CAU, consulte la sección Requisitos y mejores prácticas para el clúster: actualización compatible en technet.microsoft.com.
- Asegúrese de que el sistema operativo Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 o Windows 2019 esté instalado en todos los nodos de 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.
- Habilite una regla de firewall que permita el apagado remoto en cada nodo del clúster de conmutación por error.
- Asegúrese de que el grupo de clústeres tenga un mínimo de dos nodos.

NOTA:

- Para obtener más información acerca de cómo aplicar las actualizaciones, consulte [Actualizar y revertir versiones de firmware mediante el método Ejecutar actualización](#).
- Para obtener información acerca de Dell EMC Repository Manager para descargar actualizaciones de firmware y controladores, consulte la página *Catálogo de actualizaciones de firmware y controladores para las soluciones Dell EMC para Microsoft Azure Stack HCI* en [dell.com\support](https://dell.com/support) y descargue el archivo de catálogo.

Administrar dispositivos en OMIMSSC

Mantenga actualizados los servidores y sistemas modulares programando trabajos de actualización de firmware para componentes de servidores y sistemas modulares. Administre servidores mediante la recuperación de servidores a un estado anterior exportando su configuración anterior, aplicando las configuraciones del antiguo componente en el componente de reemplazo y exportando registros de LC para solucionar problemas.

Temas:

- [Recuperación de un servidor](#)
- [Aplicar ajustes de configuración y firmware en componente de reemplazo](#)
- [Recopilar registros de LC para servidores](#)
- [Exportar inventario](#)
- [Cancelar trabajos programados](#)

Recuperación de un servidor

Guarde las configuraciones de un servidor en un almacén de protección exportando las configuraciones a un perfil e importando el perfil en el mismo servidor para restituirlo a un estado anterior.

Almacén de protección

Un almacén de protección es un lugar seguro donde puede guardar perfiles de servidor. Exporte un perfil de servidor desde un servidor o grupo de servidores e impórtelos al mismo servidor o grupo de servidores. Puede guardar este perfil de servidor en una ubicación compartida de la red creando un almacén externo o en una tarjeta vFlash Secure Digital (SD) creando un almacén interno. Puede asociar un servidor o grupo de servidores con solo un almacén de protección. Sin embargo, puede asociar un almacén de protección con muchos servidores o grupos de servidores. Puede guardar un perfil de servidor con solo un almacén de protección. Sin embargo, puede guardar cualquier cantidad de perfiles de servidor en un único almacén de protección.

Creación del almacén de protección

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

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

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

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento > Configuración de mantenimiento > Vault de protección**.
2. Para modificar el vault, selecciónelo y haga clic en **Editar**.

NOTA: Si se modifica el vault de protección mientras los trabajos de exportación o importación de perfil de servidor están en curso, la información editada se considerará para las subtareas pendientes en el trabajo.

Eliminación del almacén de protección

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, a continuación, elimine el almacén de protección.

- Hay un trabajo programado que está asociado con almacén de protección. Sin embargo, para eliminar dicho almacén de protección, elimine el trabajo programado y, a continuación, elimine el almacén de protección.

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento > Configuración de mantenimiento > Vault de protección**.
2. Seleccione el almacén que desea eliminar y haga clic en **Eliminar**.

Exportación de perfiles de servidor

Exporte un perfil de servidor, incluidas las imágenes de firmware instaladas en distintos componentes, como BIOS, RAID, NIC, iDRAC, Lifecycle Controller y la configuración de dichos componentes. El dispositivo de OMIMSSC crea un archivo que contiene todas las configuraciones y que puede guardar en una tarjeta vFlash SD o en un recurso compartido de red. Seleccione un almacén de protección de su preferencia para guardar este archivo. Puede exportar los perfiles de configuración de un servidor o grupo de servidores inmediatamente o programar la exportación para más tarde. Además, puede seleccionar una opción de repetición pertinente para la frecuencia con la cual se deben exportar los perfiles de servidor.

Deshabilite la opción **Indicador de F1/F2 en caso de error** en **Configuración del BIOS**.

Tenga en cuenta lo siguiente antes de exportar perfiles del servidor:

- En una instancia, puede programar solo un trabajo de exportación de configuración para un grupo de servidores.
- No puede realizar ninguna otra actividad en el servidor o grupo de servidores cuyos perfiles de configuración está exportando.
- Asegúrese de que el trabajo **Copia de seguridad automática** en iDRAC no esté programado para ese mismo momento.
- No puede exportar perfiles de servidor si se aplican los filtros. Para exportar perfiles de servidor, borre todos los filtros aplicados.
- Para exportar perfiles de servidor, asegúrese de que cuenta con una licencia empresarial de iDRAC.
- Antes de exportar un perfil de servidor, asegúrese de que la dirección IP del servidor no haya cambiado. Si la dirección IP del servidor cambió debido a cualquier otra operación, entonces vuelva a descubrir este servidor en OMIMSSC y, luego, programe el trabajo de exportación de perfil de servidor.

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione los servidores cuyos perfiles desea exportar y haga clic en **Exportar** desde el menú desplegable **Perfil de dispositivo**. Aparecerá la página **Exportar perfil de servidor**.
2. En la página **Exportar perfil de servidor**, proporcione los detalles del trabajo y, luego, seleccione un almacén de protección. Para obtener más información acerca de los almacenes de protección, consulte [Creación de un almacén de protección](#).

En **Programar exportación de perfil de servidor**, seleccione una de las opciones siguientes:

- **Ejecutar ahora:** exporte inmediatamente la configuración de servidor de los servidores o grupos de servidores seleccionados.
- **Programar:** proporcione un programa para exportar la configuración de servidor del grupo de servidores seleccionado.
 - **Nunca:** seleccione esta opción para exportar el perfil de servidor solo una vez durante la hora programada.
 - **Una vez a la semana:** seleccione esta opción para exportar el perfil de servidor semanalmente.
 - **Una vez cada 2 semanas:** seleccione esta opción para exportar el perfil de servidor una vez cada dos semanas.
 - **Una vez cada 4 semanas:** seleccione esta opción para exportar el perfil de servidor una vez cada cuatro semanas.

Importar perfil de servidor

Puede importar un perfil de servidor anteriormente exportado para ese mismo servidor o grupo de servidores. Importar un perfil de servidor es útil para restaurar la configuración y el firmware de un servidor a un estado almacenado en el perfil.

Puede importar los perfiles de servidor de dos maneras:

- Importación rápida de perfil de servidor: le permite importar automáticamente el último perfil de servidor exportado para ese servidor. Para esta operación, no es necesario que seleccione perfiles de servidor individuales para cada uno de los servidores.
- Importación personalizada de perfil de servidor: le permite importar perfiles de servidor para cada uno de los servidores seleccionados individualmente. Por ejemplo, si se programó la exportación del perfil de servidor y si dicho perfil se exporta todos los días, esta función le permite seleccionar un perfil de servidor específico para que se importe desde 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 de servidor desde una lista de perfiles de servidor exportados solo para ese servidor. No puede importar los mismos perfiles de servidor para diferentes servidores o grupos de servidores. Si intenta importar un perfil de servidor de otro servidor o grupo de servidor, el trabajo de importación de perfil de servidor fallará.
 - 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 en ese servidor o grupo de servidores en particular, el trabajo de importación de perfil de servidor fallará en aquellos servidores que tengan perfil de servidor. Se agrega un mensaje de registro en los registros de actividad, el cual incluye los detalles de la falla.
 - Después de exportar un perfil de servidor, si se elimina algún componente del servidor y, luego, se da inicio a un trabajo de importación de perfil, se restauran toda la información de los componentes, excepto la información de los componentes faltantes, la cual se omite. Esta información no está disponible en el registro de actividad de OMIMSSC. Para conocer más acerca de los componentes faltantes, consulte el **registro de LifeCycle** de iDRAC.
 - No puede importar un perfil de servidor después de aplicar los filtros. Para importar perfiles de servidor, borre todos los filtros aplicados.
 - Para importar perfiles de servidor, debe tener la licencia Enterprise de iDRAC.
1. En OMIMSSC, dentro del **Centro de mantenimiento**, seleccione los servidores cuyos perfiles desea importar y haga clic en **Importar** desde el menú desplegable **Perfil de dispositivo**. Aparecerá la sección **Importar perfil de servidor**.
 2. Proporcione los detalles y seleccione el **tipo de importación de perfil de servidor** que desee.

NOTA: Un perfil de servidor se exporta junto con la configuración RAID existente. Sin embargo, puede importar el perfil de servidor con o sin la configuración de RAID en el servidor o grupo de servidores. Se selecciona **Conservar los datos** de manera predeterminada para conservar la configuración RAID existente en el servidor. Deje en blanco la casilla de verificación si desea aplicar la configuración de RAID almacenada en el perfil de servidor.
 3. Para importar el perfil de servidor, haga clic en **Completar**.

Aplicar ajustes de configuración y firmware en componente de reemplazo

La función Reemplazo de piezas actualiza automáticamente un componente de servidor de reemplazo con la versión de firmware requerida, la configuración del componente antiguo o ambos. La actualización se produce automáticamente cuando reinicia el servidor luego de reemplazar el componente.

Para establecer las configuraciones para el reemplazo de piezas:

1. En OMIMSSC, haga clic en **Centro de mantenimiento**, seleccione los servidores o el grupo de servidores y, luego, haga clic en **Reemplazo de piezas**.

NOTA: El nombre de opción se expande a **Configurar reemplazo de piezas** cuando pasa el cursor sobre **Reemplazo de piezas**.

Aparecerá la ventana **Configuración de reemplazo de piezas**.

2. Puede configurar **CSIOR**, **Actualización de firmware de pieza** y **Actualización de configuración de pieza** con cualquiera de las siguientes opciones; luego, haga clic en **Completar**:
 - Recopilación de inventario del sistema al reiniciar (CSIOR): recopila toda la información del componente en cada reinicio del sistema.
 - **Activado:** la información sobre el inventario de software y hardware de los componentes del servidor se actualiza automáticamente durante cada reinicio del sistema.
 - **Desactivado:** la información sobre el inventario de software y hardware de los componentes del servidor no se actualizan.

- **No cambiar el valor en el servidor:** se conserva la configuración del servidor existente.
- Actualización de firmware de piezas: restaura, actualiza o degrada la versión de firmware del componente según la selección que realice.
 - **Desactivado:** la actualización del firmware de la pieza está deshabilitada, al igual que el componente de reemplazo.
 - **Permitir solo la actualización de versión:** las versiones de firmware actualizadas se aplican en el componente de reemplazo siempre que la versión de firmware del nuevo componente sea anterior a la versión existente.
 - **Coincidir con el firmware de la pieza de reemplazo:** la versión de firmware del componente nuevo coincide con la versión de firmware del componente original.
 - **No cambiar el valor en el servidor:** se conserva la configuración actual del componente.
- Actualización de configuración de piezas: restaura o actualiza la configuración del componente según la selección que realice.
 - **Desactivado:** la actualización de la configuración de la pieza está deshabilitada y la configuración guardada del antiguo componente no se aplica al componente de reemplazo.
 - **Aplicar siempre:** la actualización de la configuración de la pieza está activada y la configuración guardada del antiguo componente se aplica al componente de reemplazo.
 - **Aplicar solo si coincide el firmware:** la configuración guardada del antiguo componente se aplica al componente de reemplazo solo si sus versiones de firmware coinciden.
 - **No cambiar el valor en el servidor:** se conserva la configuración existente.

Recopilar registros de LC para servidores

Los registros de LC proporcionan registros de actividades pasadas en un servidor administrado. Estos archivos de registro son útiles para los administradores de 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 disponible en los registros de LC: información relacionada con alertas, cambios de configuración en los componentes de hardware del sistema, cambios del firmware debido a una actualización o degradación, piezas reemplazadas, advertencias de temperatura, registros detallados de fecha y hora del momento en el que se inició la actividad, gravedad de la actividad, etc.

El archivo de registro exportado de LC se guarda en una carpeta cuyo nombre es el de la etiqueta de servicio del servidor. Los registros de LC se guardan en el formato: <YYYYMMDDHHMMSSSS>.<file format>. 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.

Existen dos opciones para recopilar registros de LC:

- Registros de LC completos: exporta archivos de registro de LC activos y archivados. Son archivos de gran tamaño. Por ende, están comprimidos en el formato .gz y se exportan a la ubicación especificada en un recurso compartido de red CIFS.
- Registros de LC activos: exporta archivos de registro LC recientes de forma inmediata o programa un trabajo para exportar los archivos de registro en intervalos regulares. Vea estos archivos de registro, búsquelos y expórtelos al dispositivo OMIMSSC. Además, puede guardar un respaldo de los archivos de registro en un recurso compartido de red.

Para recopilar registros de LC, realice los pasos siguientes:

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione un servidor o grupo de servidores, haga clic en el menú desplegable **Registros de LC** y, luego, haga clic en **Recopilar registros de LC**.
2. En **Recopilación de registros de LC**, seleccione una de las siguientes opciones y haga clic en **Completar**:
 - **Exportar registros de LC completos (.gz):** seleccione esta opción para exportar registros de LC completos a un recurso compartido de red CIFS proporcionando credenciales de Windows.
 - **Exportar registros activos (Ejecutar ahora):** seleccione esta opción para exportar los registros activos inmediatamente al dispositivo OMIMSSC.
 - (Opcional) Seleccione la casilla de verificación **Respaldo los registros de LC en el recurso compartido de red** para guardar un respaldo de los registros de LC en el recurso compartido de red CIFS proporcionando las credenciales de Windows.
 - **Programar recopilación de registros de LC:** seleccione esta opción para exportar los registros activos en intervalos regulares.

En **Programar recopilación de registros de LC**, seleccione una fecha y hora para exportar los archivos de registro.

Seleccione un botón de opción según la frecuencia con la que se deben exportar los archivos. Las opciones disponibles para programar la frecuencia y determinar la frecuencia con la que desea recopilar los registros de LC son:

- **Nunca:** esta opción está seleccionada de manera predeterminada. Seleccione esta opción para exportar los registros de LC solo una vez a la hora programada.

- **Diariamente:** seleccione esta opción para exportar los registros de LC diariamente a la hora programada.
- **Una vez a la semana:** seleccione esta opción para exportar los registros de LC una vez a la semana a la hora programada.
- **Una vez cada 4 semanas:** seleccione esta opción para exportar los registros de LC una vez cada cuatro semanas a la hora programada.
- (Opcional) Seleccione la casilla de verificación **Respaldo los registros de LC en el recurso compartido de red** para guardar un respaldo de los registros de LC en el recurso compartido de red CIFS proporcionando las credenciales de Windows.

NOTA: Tenga a mano una carpeta de recurso compartido con suficiente espacio de almacenamiento, ya que los archivos exportados son de gran tamaño.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Ver registros de LC

Vea todos los registros activos de LC, busque descripciones detalladas y descargue los registros en formato CSV.

Agregue el dispositivo OMIMSSC en la lista **Sitio de intranet local** como se indica en la sección *Configuración del navegador* en la *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*.

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione un servidor o grupo de servidores, haga clic en el menú desplegable **Registros de LC** y, luego, en **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 un nombre de archivo para ver todas las entradas de registro en el archivo de registro de LC específico de ese servidor. Para obtener más información, consulte [Descripción de 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 del mensaje en un archivo LC:

- Haga clic en un nombre de archivo para abrir el archivo de registro de LC y busque una descripción en el cuadro de búsqueda.
- Ingrese un texto de descripción en el cuadro de búsqueda y, luego, vea todos los archivos de LC con estas instancias de texto.

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

NOTA: El tiempo que se muestra en los mensajes de registro de LC sigue la zona horaria del iDRAC.

Descripción de archivo

Utilice esta página para ver información detallada sobre las acciones que se recomiendan y demás información técnica que es útil para realizar seguimiento o crear alertas para un servidor en particular.

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

- Puede buscar descripciones de mensajes en particular.
- Puede ver los archivos de registro en la ventana o descargar el archivo para ver más mensajes de registro.
- Puede ver cualquier comentario escrito por un usuario para una actividad.

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

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

NOTA: Haga clic en **ID de mensaje** para ver más información acerca del mensaje.

Exportar inventario

Exporte el inventario de servidores seleccionados o de un grupo de servidores a un archivo con formato XML o CSV. Puede guardar esta información en un directorio compartido Windows o en un sistema de administración. Utilice esta información de inventario para crear un archivo de inventario de referencia en un origen de actualización.

Asegúrese de establecer la configuración del navegador como se indica en la sección *Configuración del navegador* en la *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*.

NOTA: Puede importar el archivo XML en DRM y crear un repositorio basado en el archivo de inventario.

NOTA: Aunque solo seleccione la información del componente de un servidor y la exporte, la información de inventario del servidor se exporta en su totalidad.

1. En **OMIMSSC**, haga clic en **Centro de mantenimiento**.
2. Seleccione los servidores cuyo inventario desea exportar y seleccione el formato en el menú desplegable **Exportación de inventario**.

Se exporta el archivo en formato XML o CSV, según su selección. El archivo se compone de información como 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, la versión de firmware actual en ese componente, la versión del firmware desde el origen de actualización y la acción de actualización en ese componente.

Cancelar trabajos programados

Asegúrese de que el trabajo se encuentre en el estado **Programado**.

1. En OMIMSSC, realice cualquiera de las siguientes tareas:
 - En el panel de navegación, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Administrar tareas**.
 - En el panel de navegación, haga clic en **Centro de tareas y registros** y, a continuación, haga clic en la pestaña **Programado**.
2. Seleccione los trabajos que desea cancelar, haga clic en **Cancelar** y, luego, en **Sí** para confirmar.

Aprovisionamiento de dispositivos desde OMIMSSC OMIMSSC

En este capítulo, se incluye información detallada acerca del descubrimiento de dispositivos Dell EMC, la implementación del sistema operativo, la creación de clústeres y el mantenimiento de estos dispositivos mediante OMIMSSC.

Temas:

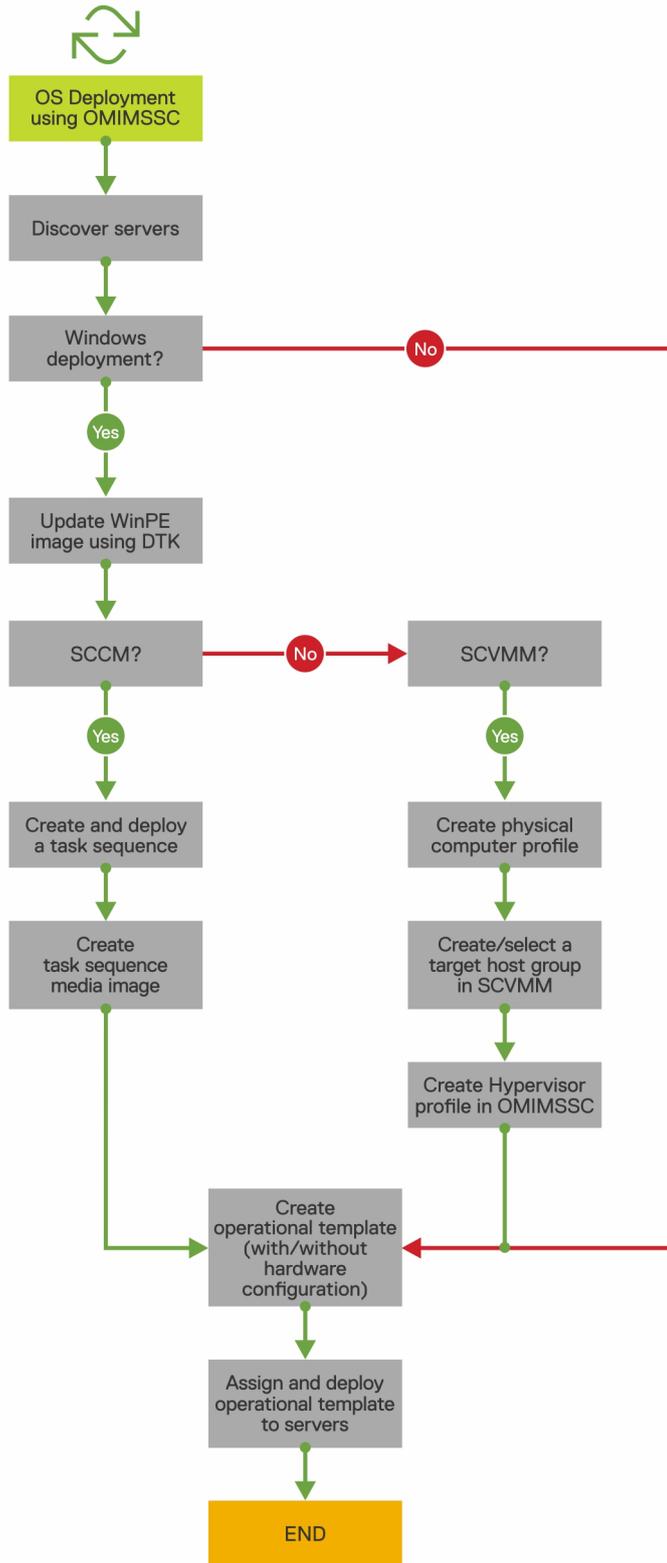
- [Flujo de trabajo para escenarios de implementación](#)
- [Crear clústeres de Storage Spaces Direct mediante Plantilla operativa predefinidas](#)
- [Flujo de trabajo para el mantenimiento de dispositivos](#)

Flujo de trabajo para escenarios de implementación

Utilice OMIMSSC para implementar el sistema operativo Windows y otros sistemas distintos en entornos SCCM o SCVMM mediante Plantilla operativa.

 **NOTA:** Asegúrese de actualizar las versiones del firmware del dispositivo a las últimas versiones disponibles en ftp.dell.com o downloads.dell.com antes de implementar el sistema operativo.

A continuación, se muestra una representación gráfica de los casos de uso de implementación del sistema operativo en



OMIMSSC.

Implementación de un sistema operativo Windows mediante la extensión de la consola de OMIMSSC para SCCM

Para implementar el SO Windows a través de la consola de SCCM utilizando OMIMSSC, realice los pasos siguientes:

NOTA: Antes de implementar el SO en un servidor host, asegúrese de que en SCCM, el estado **Cliente** del servidor sea **No**.

1. Descargue la versión más reciente de Dell EMC Deployment ToolKit (DTK) y cree una imagen WIM de arranque del entorno de preinstalación de Windows (WinPE). Para obtener más información, consulte [Actualización de WinPE](#).
2. Importe esta imagen .WIN 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 con SCCM. Para obtener más información, consulte [Crear una secuencia de tareas](#).
4. Cree una imagen de medios para secuencia de tareas en SCCM. Para obtener más información, consulte la *documentación de Microsoft*.

NOTA: Para activar una implementación desatendida del SO cuando crea un medio de secuencia de tareas, en **Seleccione el tipo de medio**, seleccione la casilla de verificación **Permitir implementación desatendida del sistema operativo**.

5. Descubra el servidor de referencia mediante la página **Descubrimiento**. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento manual](#).
6. Cree una Plantilla operativa mediante la captura de todos los detalles del servidor descubierto. Para obtener más información, consulte [Crear plantilla operativa a partir de servidores de referencia](#).
7. Asigne una Plantilla operativa en el dispositivo administrado y compruebe si la plantilla es compatible. Para obtener más información, consulte [Asignar una plantilla operativa y evaluar la compatibilidad de la plantilla operativa](#).
8. Implemente una plantilla operativa para que la plantilla del dispositivo sea compatible. Para obtener más información, consulte [Implementar plantilla operativa](#).
9. Vea el estado del trabajo de implementación del sistema operativo en la página **Centro de trabajos y registros**. Para obtener más información, consulte [Abrir el centro de trabajos y registros](#).

Implementación de un hipervisor mediante la extensión de la consola de OMIMSSC para SCVMM

Los siguientes son los diferentes escenarios para la implementación de hipervisores:

Tabla 10. Escenarios de implementación de hipervisores

Estado	Acción
Si necesita los controladores de fábrica más recientes.	Cuando cree un perfil de hipervisor, active la inyección de controlador de Lifecycle Controller (LC).
Si desea conservar la configuración de hardware existente.	Cuando cree la Plantilla operativa, desmarque la casilla de verificación para todos los componentes que no requieren ningún cambio.

Para implementar un hipervisor mediante la consola de SCVMM utilizando OMIMSSC, realice los pasos siguientes:

1. Descargue la versión más reciente de Dell EMC Deployment ToolKit (DTK) y cree una imagen ISO de arranque del entorno de preinstalación de Windows (WinPE). Para obtener más información, consulte [Actualización de WinPE](#).
2. Cree un perfil del equipo físico y un grupo de hosts en SCVMM. Para obtener más información, consulte la documentación de SCVMM.
3. Cree un perfil de hipervisor en la extensión de la consola de OMIMSSC para SCVMM. Para obtener más información, consulte [Crear un perfil de hipervisor](#).
4. Descubra el servidor de referencia mediante la página Descubrimiento. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento manual](#).
5. Cree una plantilla operativa mediante la captura de todos los detalles del servidor descubierto. Para obtener más información, consulte [Crear plantilla operativa a partir de servidores de referencia](#).
6. Asigne una plantilla operativa en el dispositivo administrado y compruebe si la plantilla es compatible. Para obtener más información, consulte [Asignar una plantilla operativa y evaluar la compatibilidad de la plantilla operativa](#).
7. Implemente una plantilla operativa para que la plantilla del dispositivo sea compatible. Para obtener más información, consulte [Implementar plantilla operativa](#).
8. Vea el estado del trabajo de implementación del sistema operativo en la página Centro de trabajos y registros. Para obtener más información, consulte [Abrir el centro de trabajos y registros](#).

Volver a implementar el sistema operativo Windows mediante OMIMSSC OMIMSSC

Para volver a implementar el SO de Windows en un servidor mediante la extensión de la consola de OMIMSSC para SCCM o la extensión de la consola de OMIMSSC en SCVMM, realice los pasos siguientes:

1. Elimine el servidor desde la consola de Microsoft. Para obtener más información, consulte la documentación de Microsoft.
2. Vuelva a detectar el servidor o sincronice OMIMSSC con la consola Microsoft registrada. El servidor se agrega como un servidor sin asignar en OMIMSSC. Para obtener más información acerca del descubrimiento, consulte [Descubrir servidores mediante el descubrimiento manual](#). Para obtener más información acerca de la sincronización, consulte [Sincronizar con consolas Microsoft inscritas](#).
3. Cree una Plantilla operativa mediante la captura de todos los detalles del servidor descubierto. Para obtener más información, consulte [Crear plantilla operativa a partir de servidores de referencia](#).
4. Asigne una Plantilla operativa en el dispositivo administrado y compruebe si la plantilla es compatible. Para obtener más información, consulte [Asignar una plantilla operativa y evaluar la compatibilidad de la plantilla operativa](#).
5. Implemente una plantilla operativa para que la plantilla del dispositivo sea compatible. Para obtener más información, consulte [Implementar plantilla operativa](#).
6. Vea el estado del trabajo de implementación del sistema operativo en la página **Centro de trabajos y registros**. Para obtener más información, consulte [Abrir el centro de trabajos y registros](#).

Implementación de un sistema operativo distinto a Windows mediante las extensiones de la consola de OMIMSSC

Para implementar un sistema operativo distinto a Windows mediante OMIMSSC, realice los pasos siguientes:

 **NOTA:** Los pasos para implementar sistemas operativos distintos a Windows mediante OMIMSSC son los mismos para ambas consolas de Microsoft.

1. Descubra el servidor de referencia mediante la página **Descubrimiento**. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento manual](#).
2. Cree una Plantilla operativa mediante la captura de todos los detalles del servidor descubierto. Para obtener más información, consulte [Crear plantilla operativa a partir de servidores de referencia](#).
3. Asigne una Plantilla operativa en el dispositivo administrado y compruebe si la plantilla es compatible. Para obtener más información, consulte [Asignar una plantilla operativa y evaluar la compatibilidad de la plantilla operativa](#).
4. Implemente una plantilla operativa para que la plantilla del dispositivo sea compatible. Para obtener más información, consulte [Implementar plantilla operativa](#).

 **NOTA:** Si la búsqueda de DHCP falla durante la implementación, el servidor agota el tiempo de espera y no se mueve a la recopilación de **Managed Dell Lifecycle Controller (ESXi)** en SCCM.

Crear clústeres de Storage Spaces Direct mediante Plantilla operativa predefinidas

Para crear clústeres mediante OMIMSSC, realice los pasos siguientes:

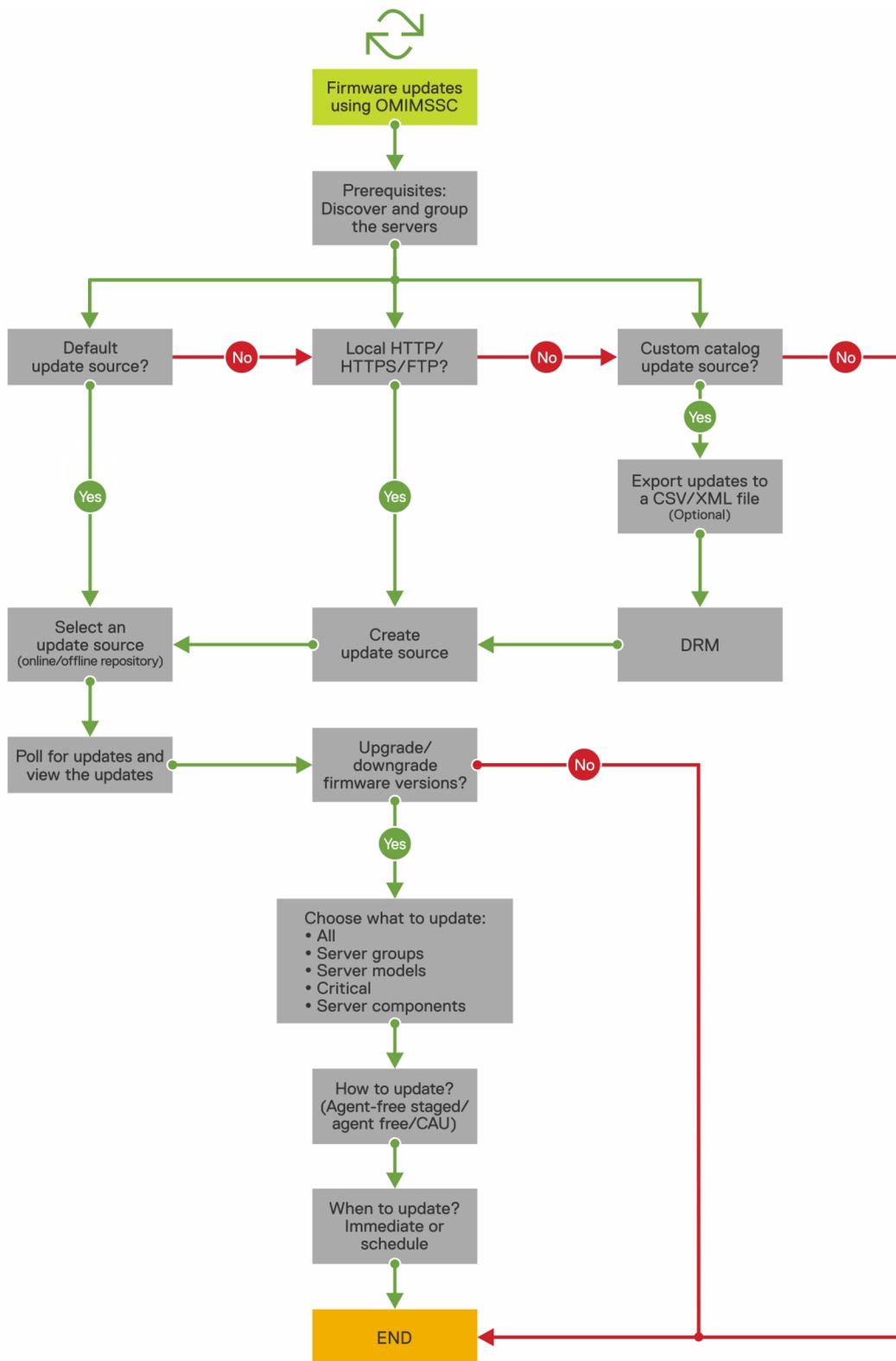
1. Descubra el servidor de referencia mediante la página **Descubrimiento**. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento manual](#).
2. Edite la Plantilla operativa predefinida. Para obtener más información, consulte [Modificar una Plantilla operativa](#).
3. Cree un switch lógico. Para obtener más información, consulte [Crear un switch lógico](#).
4. Cree un clúster de Storage Spaces Direct. Para obtener más información, consulte [Crear clústeres de Storage Spaces Direct](#).

Flujo de trabajo para el mantenimiento de dispositivos

Realice mantenimiento en los dispositivos descubiertos en OMIMSSC.

Actualizar el firmware de servidores y dispositivos MX7000

A continuación, se muestra una representación gráfica del flujo de trabajo de actualización del firmware.



Puede actualizar los dispositivos seleccionados mediante los siguientes orígenes de actualización:

- FTP en línea o fuente FTP local
- HTTP en línea o fuente HTTP local
- HTTPS en línea u origen HTTPS local
- Fuente DRM (Dell Repository Manager) local

1. Cree o seleccione un origen de actualización predeterminada. Para obtener más información acerca de los orígenes de actualización, consulte [Origen de actualización](#).

NOTA: Asegúrese de actualizar el origen de actualización con el catálogo más reciente mediante la función Sondeo y notificación. Para obtener más información acerca del sondeo y la notificación, consulte [Sondeo y notificación](#).

Si va a actualizar clústeres de Storage Spaces Direct, seleccione un origen de actualización predefinido específico para clústeres de Storage Spaces Direct. Estos orígenes de actualización solo se muestran en la página **Centro de mantenimiento**.

Si actualiza dispositivos MX7000, seleccione un origen de actualización predefinido específico para sistemas modulares. Estos orígenes de actualización solo se muestran en la página **Centro de mantenimiento**.

2. Cree o seleccione los grupos de actualización predeterminados. Para obtener más información acerca de los grupos de actualización, consulte [Grupos de actualización](#).
3. Descubra o sincronice los dispositivos con una consola Microsoft registrada y asegúrese de que el inventario de dispositivos sea el más reciente. Para obtener más información acerca del descubrimiento y la sincronización, consulte [Descubrimiento de dispositivos y sincronización](#). Para obtener más información acerca del inventario de servidor, consulte [Iniciar vista de servidor](#).
4. Actualice el dispositivo a través de una de las siguientes opciones:
 - Seleccione los dispositivos requeridos y haga clic en **Ejecutar actualización**. Para obtener más información, consulte [Actualizar o revertir versiones de firmware mediante el método Ejecutar actualización](#).
 - NOTA:** Para degradar el firmware de los componentes del dispositivo, seleccione la casilla de verificación **Permitir degradación**. Si esta opción no está seleccionada, entonces no hay una acción en el componente que exija una degradación de firmware.
 - Seleccione el componente de actualización de firmware en Plantilla operativa e implemente esta plantilla. Para obtener más información acerca de las Plantilla operativa, consulte [Plantilla operativa](#).

Configurar los componentes sustituidos

Para obtener información acerca de cómo coincidir la versión del firmware o los ajustes de configuración del componente de reemplazo con los del componente antiguo, consulte [Aplicar firmware y ajustes de configuración](#).

Exportación e importación de perfiles de servidor

Exporte el perfil de servidor en una instancia concreta y, luego, importe el perfil para restituir el servidor:

1. Cree un almacén de protección. Para obtener más información acerca de cómo crear un almacén de protección, consulte [Creación de un almacén de protección](#).
2. Exporte un perfil de servidor. Para obtener más información acerca de cómo exportar un perfil de servidor, consulte [Exportación de perfil de servidor](#).
3. Importe un perfil de servidor al mismo servidor desde el cual se exportó. Para obtener más información acerca de cómo importar un perfil de servidor, consulte [Importación de perfil de servidor](#).

NOTA: Puede importar el perfil de servidor, incluida la configuración de RAID, solo si la configuración de RAID se exporta al perfil.

Configuración e implementación

Descubrir

1. En la consola de OMIMSSC, realice uno de los pasos siguientes:
 - En el tablero, haga clic en **Descubrir servidores**.
 - En el panel de navegación, haga clic en **Configuración e implementación**, en **Vista de servidor** y, luego, en **Descubrir**.
2. Haga clic en **Detectar**.

Para ver los cambios realizados, actualice la página **Perfil de credencial**.

Temas:

- [Casos de uso](#)
- [Crear Plantillas operativas](#)
- [Carpetas del instalador](#)
- [Asignar Plantillas operativas](#)
- [Implementar Plantillas operativas](#)
- [Componente del sistema operativo Windows para la extensión de la consola de OMIMSSC para SCCM](#)
- [Componente de Windows para la extensión de la consola de OMIMSSC para SCVMM](#)
- [Componente distinto a Windows para la extensión de la consola de OMIMSSC para SCCM/SCVMM](#)
- [Descubrimiento en MSSC inscrita](#)
- [Importación del perfil del servidor](#)
- [Exportar perfil del servidor](#)
- [Ver registros de LC](#)
- [Recopilar registros de LC](#)
- [Sustitución de piezas](#)
- [Sondeo y notificación](#)
- [Iniciar iDRAC](#)
- [Iniciar módulo de entrada/salida](#)
- [Resolución de errores de sincronización](#)
- [Sincronizar OMIMSSC con consolas Microsoft inscritas](#)
- [Implementar un clúster Azure Stack HCI](#)

Casos de uso

1. Descubra el servidor de referencia mediante la página **Descubrimiento**. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento manual](#).
2. Cree una Plantilla operativa mediante la captura de todos los detalles del servidor descubierto. Para obtener más información, consulte [Crear plantilla operativa a partir de servidores de referencia](#).
3. Asigne una Plantilla operativa en el dispositivo administrado y compruebe si la plantilla es compatible. Para obtener más información, consulte [Asignar una plantilla operativa y evaluar la compatibilidad de la plantilla operativa](#).
4. Implemente una Plantilla operativa para que la plantilla del dispositivo sea compatible. Para obtener más información, consulte [Implementar plantilla operativa](#).
5. Vea el estado del trabajo de implementación del sistema operativo en la página **Centro de trabajos y registros**. Para obtener más información, consulte [Abrir el centro de trabajos y registros](#).

Crear Plantillas operativas

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

- Descubra un servidor de referencia mediante la función **Descubrimiento**. Para obtener más información acerca de cómo descubrir servidores, consulte [Descubrir servidores mediante el descubrimiento manual](#).
- Descubra un sistema modular mediante la función **Descubrimiento**. Para obtener más información acerca de cómo descubrir sistemas modulares, consulte [Descubrir sistemas modulares mediante el descubrimiento manual](#).
- Si no utiliza el origen de actualización predeterminado, entonces cree un origen de actualización. Para obtener más información, consulte [Crear un origen de actualización](#).
- Para usuarios de SCCM:
 - Cree una secuencia de tareas. Para obtener más información, consulte [Crear una secuencia de tareas](#).
 - Para implementar un sistema operativo distinto a Windows, debe tener un perfil de credencial de tipo dispositivo. Para obtener más información, consulte [Crear un perfil de credencial](#).
- Para usuarios de SCVMM:
 - Cree un perfil de hipervisor. Para obtener información acerca de cómo crear un perfil de hipervisor, consulte [Crear perfil de hipervisor](#).
 - Para implementar Windows, debe tener un perfil de credencial de tipo dispositivo. Para obtener más información, consulte [Crear un perfil de credencial](#).

1. En OMIMSSC, realice alguno de los siguientes pasos para abrir una Plantilla operativa:

- En el panel de OMIMSSC, haga clic en **Crear plantilla operativa**.
- En el panel de navegación, haga clic en **Perfiles > Plantilla operativa** y, luego, en **Crear**.

Aparece el asistente **Plantilla operativa**.

2. Haga clic en **Crear**.

Aparece el asistente **Plantilla operativa**.

3. Ingrese un nombre y una descripción para la plantilla.

4. Seleccione el tipo de dispositivo, ingrese la dirección IP del dispositivo de referencia y, luego, haga clic en **Siguiente**.

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

5. En **Componentes del dispositivo**, haga clic en un componente para ver los atributos disponibles y sus valores.

A continuación, se enumeran los componentes:

- Actualización del firmware
- Componentes de hardware, los cuales son RAID, NIC y BIOS.

i **NOTA:** En el componente **iDRAC integrado 1**, verá los siguientes privilegios y sus valores para el atributo **Privilegio de usuario administrador**.

Tabla 11. Tabla de valores de privilegio

Valor	Privilegio
1	Inicio de sesión
2	Configurar
4	Configurar usuarios
8	Registros
16	Control del sistema
32	Acceder a la consola virtual
64	Acceder a los medios virtuales
128	Operaciones del sistema
256	Depuración
499	Privilegios de operador

- Sistema operativo: seleccione Windows, ESXi o RHEL.

6. Utilice la barra de desplazamiento horizontal para localizar un componente. Seleccione el componente, expanda un grupo y, luego, edite sus valores de atributo. Utilice la barra de desplazamiento vertical para editar los grupos y atributos de un componente.

7. Seleccione la casilla de verificación en cada uno de los componentes, ya que las configuraciones de los componentes seleccionados se aplican en el dispositivo administrado cuando se aplica la Plantilla operativa. Sin embargo, todas las configuraciones del dispositivo de referencia se capturan y guardan en la plantilla.

 **NOTA:** Sin importar que selección realice en la casilla de verificación de cada componente, todas las configuraciones se capturan en la plantilla.

En el componente **Sistema operativo**, realice los pasos que se indican en cualquiera de las opciones siguientes, según sus requisitos:

- Para implementar el sistema operativo Windows en SCCM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCCM](#).
- Para implementar el sistema operativo Windows en SCVMM, consulte [Componente Windows para la extensión de la consola de OMIMSSC para SCVMM](#).
- OMIMSSC
- Para implementar un sistema operativo distinto a Windows, consulte [Componente distinto a Windows para las extensiones de la consola de OMIMSSC](#).

8. Para guardar el perfil, haga clic en **Completar**.

Carpetas del instalador

Las siguientes carpetas se crean después de instalar la extensión de consola:

- Registro: esta carpeta contiene información de registro relacionada con la consola.

 **NOTA:** Si las credenciales para la cuenta de administrador del dominio y la cuenta de administrador local son diferentes, no utilice la cuenta de administrador del dominio para iniciar sesión en SCCM o SCVMM. En vez de esto, utilice una cuenta de usuario de dominio diferente para iniciar sesión en SCCM o SCVMM.

Asignar Plantillas operativas

1. En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de servidor**. Seleccione los servidores necesarios y haga clic en **Asignar plantilla operativa y evaluar compatibilidad**.
Aparece la página **Asignar Plantilla operativa y evaluar compatibilidad**.
2. Seleccione los servidores necesarios y haga clic en **Asignar plantilla operativa y evaluar compatibilidad**.
3. En OMIMSSC, haga clic en **Configuración e implementación** y en **Vista de sistemas modulares**. Seleccione el sistema modular necesario y haga clic en **Asignar plantilla operativa**.
Aparece la página **Asignar Plantilla operativa**.
4. Seleccione los sistemas modulares necesarios y haga clic en **Asignar plantilla operativa y evaluar compatibilidad**.
Aparece la página **Asignar Plantilla operativa**.
5. Seleccione la plantilla en el menú desplegable **Plantilla operativa**, ingrese un nombre de trabajo y, luego, haga clic en **Asignar**.

El menú desplegable Plantilla operativa enumera las plantillas del mismo tipo que el de los dispositivos seleccionados en el paso anterior.

Si el dispositivo es compatible con la plantilla, entonces aparece una casilla de color **verde** con una marca de verificación.

Si la Plantilla operativa no se aplica correctamente en el dispositivo o si el componente de hardware en Plantilla operativa no está seleccionado, entonces aparece una casilla con el símbolo de **información**.

Si el dispositivo no es compatible con la plantilla, entonces aparece una casilla con el símbolo de **advertencia**. Únicamente si el dispositivo no es compatible con la Plantilla operativa asignada, puede ver un informe de resumen haciendo clic en el enlace del nombre de la plantilla. La página **Informe de resumen de compatibilidad de Plantilla operativa** muestra un informe de resumen de las diferencias entre la plantilla y el dispositivo.

Para ver un informe detallado, realice los pasos siguientes:

- a. Haga clic en **Ver compatibilidad detallada**. Aquí se muestran los componentes cuyos valores de atributos son distintos a los valores de la plantilla asignada. Los colores indican los diferentes estados de compatibilidad de la Plantilla operativa.
 - Símbolo de advertencia de color amarillo: incompatible. Indica que la configuración del dispositivo no coincide con los valores de plantilla.

- Recuadro de color rojo: indica que el componente no está presente en el dispositivo.

Implementar Plantillas operativas

NOTA: Asegúrese de que no habilitar atributos que cambien las credenciales para iniciar sesión en el dispositivo después de implementar la Plantilla operativa.

1. En OMIMSSC, haga clic en **Configuración e implementación** y haga clic en **Vista de servidor**. Seleccione los servidores en los que aplicó la plantilla y, luego, haga clic en **Implementar Plantilla operativa**. Aparecerá el asistente **Implementar Plantilla operativa**.
2. En OMIMSSC, haga clic en **Configuración e implementación** y en **Vista de sistemas modulares**. Seleccione el sistema modular en el cual asignó la plantilla y, luego, haga clic en **Implementar Plantilla operativa**. Aparecerá el asistente **Implementar Plantilla operativa**.
3. (Opcional) Para exportar todos los atributos marcados como valores de pool en la plantilla seleccionada a un archivo .CSV, haga clic en **Exportar atributos de pool**; de lo contrario, vaya al paso 4.

NOTA: Antes de exportar los valores de pool, agregue al sitio de intranet local la dirección IP del dispositivo OMIMSSC en el que está instalada la extensión de la consola de OMIMSSC. Para obtener más información acerca de cómo agregar la dirección IP en el navegador Internet Explorer, consulte la sección *Configuración del navegador* en *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*.

4. Si exportó los valores de pool, ingrese valores para todos los atributos que se marcan como valores de pool en el archivo .CSV y guarde el archivo. En **Pool de valor de atributo**, seleccione este archivo para importarlo.

El formato de un archivo .CSV es `attribute-value-pool.csv attribute-value-pool.csv`

NOTA: Asegúrese de seleccionar un archivo .CSV que tenga todos los atributos correspondientes y que no cambien ni la IP de iDRAC ni las credenciales de iDRAC debido a la plantilla, puesto que OMIMSSC deja de hacer seguimiento del trabajo después de que la IP de iDRAC o las credenciales de iDRAC cambian y se marca como fallido a pesar de que el trabajo se realice correctamente en iDRAC.

5. Ingrese un nombre de trabajo único y una descripción para el trabajo, y haga clic en **Implementar**. Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

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

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

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

Para obtener más información acerca de la secuencia de tareas, consulte [Secuencia de tareas](#).

2. Seleccione una de las siguientes opciones para el **método de implementación**:

- **Arrancar en ISO de red:** reinicia la ISO especificada.
- **Colocar ISO en vFlash y reiniciar:** descarga la imagen ISO en vFlash y reinicia.
- **Reiniciar en vFlash:** reinicia en vFlash. Asegúrese de que la imagen ISO esté presente en vFlash.

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

3. (Opcional) Para utilizar la imagen presente en el recurso compartido de red, seleccione la opción **Utilizar ISO de red como alternativa**.
4. Ingrese un archivo de imagen de medios de arranque LC.
5. Seleccione los controladores necesarios para el sistema operativo.

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

Seleccione **Perfil de hipervisor**, **Perfil de credencial** y **Origen de IP de servidor**.

NOTA: **Nombre de host** y **NIC de administración de servidor** siempre son valores de pool. En el caso de una NIC de administración de servidores, proporcione la dirección MAC del puerto de red a través del cual desea que el sistema operativo se comunique con SCVMM.

Si selecciona **Origen de IP de servidor** como **Estático**, entonces asegúrese de haber configurado la red lógica en SCVMM y que los siguientes campos sean valores de pool:

- **Red lógica de consola**
- **Subred IP**
- **Dirección IP estática**

Componente distinto a Windows para la extensión de la consola de OMIMSSC para SCCM/SCVMM

Seleccione un sistema operativo distinto a Windows, la versión del sistema operativo, el tipo de carpeta de recurso compartido, el nombre del archivo ISO, la ubicación del archivo ISO y la contraseña de la cuenta root del sistema operativo.

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

Nombre de host es un valor de pool y si desactiva la opción DHCP, entonces los siguientes campos serán valores de pool:

- **Dirección IP**
- **Máscara de subred**
- **Puerta de enlace predeterminada**
- **DNS primario**
- **DNS secundario**

NOTA: Los tipos de recurso compartido NFS (Sistema de archivos de red) y CIFS (Sistema de archivos de Internet común) son compatibles para la implementación de un sistema operativo distinto a Windows.

Descubrimiento en MSSC inscrita

Después del descubrimiento, el servidor se agrega a la pestaña **Hosts** o a la pestaña **Sin asignar**. Además, el servidor detectado se marca como compatible o incompatible cuando tiene las versiones mínimas de firmware de LC, iDRAC y BIOS necesarias para trabajar con OMIMSSC.

- Cuando detecta un servidor PowerEdge que cuenta con un sistema operativo y que ya está presente en la consola SCCM o SCVMM, entonces el servidor aparece como un servidor host en la pestaña **Hosts** de la consola OMIMSSC cuando se inicia el trabajo de detección.
 - Si el host es un servidor modular, también se muestra la etiqueta de servicio del sistema modular que contiene al servidor.
 - Si el host forma parte de un clúster, se muestra el nombre de dominio calificado (FQDN) del clúster.
- Cuando detecta un servidor PowerEdge que no aparece en SCCM o SCVMM, entonces el servidor aparece en la lista como un servidor sin asignar en la pestaña **Sin asignar** de todas las consolas OMIMSSC inscritas.
- Después de descubrir un servidor, se consume una licencia. El conteo de **nodos de licencia** disminuye junto con la cantidad de licencias descubiertas.

Importación del perfil del servidor

1. En OMIMSSC, dentro del **Centro de mantenimiento**, seleccione los servidores cuyos perfiles desea importar y haga clic en **Importar** desde el menú desplegable **Perfil de dispositivo**. Aparecerá la sección **Importar perfil de servidor**.

2. Seleccione los servidores cuyos perfiles desea importar y haga clic en **Importar** desde el menú desplegable **Perfil de dispositivo**.
Aparecerá la sección **Importar perfil de servidor**.

Exportar perfil del servidor

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione los servidores cuyos perfiles desea exportar y haga clic en **Exportar** desde el menú desplegable **Perfil de dispositivo**.
Aparecerá la página **Exportar perfil de servidor**.
2. Seleccione los servidores cuyos perfiles desea exportar y haga clic en **Exportar** desde el menú desplegable **Perfil de dispositivo**.
Aparecerá la página **Exportar perfil de servidor**.

Ver registros de LC

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione un servidor o grupo de servidores, haga clic en el menú desplegable **Registros de LC** y, luego, en **Ver registros de LC**.
2. Seleccione los servidores cuyos registros desea ver, haga clic en el menú desplegable **Registros de LC** y, luego, en **Ver registros de LC**.

Recopilar registros de LC

1. En OMIMSSC, haga clic en **Centro de mantenimiento**. Seleccione un servidor o grupo de servidores, haga clic en el menú desplegable **Registros de LC** y, luego, haga clic en **Recopilar registros de LC**.
2. Seleccione los servidores cuyos registros desea exportar; después, haga clic en el menú desplegable **Registros de LC** y, luego, en **Recopilar registros de LC**.

Sustitución de piezas

1. En OMIMSSC, haga clic en **Centro de mantenimiento**, seleccione los servidores o el grupo de servidores y, luego, haga clic en **Reemplazo de piezas**.

 **NOTA:** El nombre de opción se expande a **Configurar reemplazo de piezas** cuando pasa el cursor sobre **Reemplazo de piezas**.

Aparecerá la ventana **Configuración de reemplazo de piezas**.

2. Seleccione los servidores cuyo componente desea configurar y, luego, haga clic en **Reemplazo de piezas**.

 **NOTA:** El nombre de opción se expande a **Configurar reemplazo de piezas** cuando pasa el cursor sobre **Reemplazo de piezas**.

Aparecerá la ventana **Configuración de reemplazo de piezas**.

Sondeo y notificación

1. En OMIMSSC, haga clic en **Centro de mantenimiento** y, luego, en **Sondeo y notificación**.
2. Haga clic en **Sondeo y notificación**.

Iniciar iDRAC

1. En OMIMSSC, expanda **Configuración e implementación** y seleccione una de las siguientes opciones:
 - Haga clic en **Vista de servidor**. Según el servidor (si se trata de un host o un servidor sin asignar), haga clic en la pestaña **Servidores sin asignar** o **Hosts**; luego, haga clic en la dirección **IP de iDRAC** del servidor.

La pestaña **Servidores sin asignar** se muestra de manera predeterminada.

Para ver la pestaña Hosts, haga clic en **Hosts**.

- Haga clic en **Vista de clúster**. Expanda el tipo de clúster y expanda el grupo de clúster a nivel de servidor. Aparece la pestaña **Servidor**.

2. Para iniciar la consola de iDRAC, haga clic en la **dirección IP**.
3. Para iniciar la consola de iDRAC, haga clic en la **dirección IP**.

Iniciar módulo de entrada/salida

Para iniciar la consola Módulo de Entrada/Salida, realice los pasos siguientes:

1. En OMIMSSC, expanda **Configuración e implementación** y haga clic en **Vista de sistemas modulares**. Expanda el modelo a nivel de dispositivos individuales. Se muestran todos los dispositivos con ese modelo.
2. Haga clic en la pestaña **Módulos de E/S**.
3. Haga clic en la **dirección IP** del dispositivo.

Resolución de errores de sincronización

1. En OMIMSSC, haga clic en **Configuración e implementación**, haga clic en **Vista de servidor** y, luego, en **Resolver errores de sincronización**.
2. Haga clic en **Resolver errores de sincronización**.

Sincronizar OMIMSSC con consolas Microsoft inscritas

1. En OMIMSSC, haga clic en **Configuración e implementación**, haga clic en **Vista de servidor** y, luego, en **Sincronizar con OMIMSSC** para sincronizar todos los hosts que aparecen en la MSSC inscrita con el dispositivo OMIMSSC.
2. Para sincronizar todos los hosts que aparecen en la MSSC inscrita con el dispositivo, haga clic en **Sincronizar con OMIMSSC**.
La sincronización es una tarea cuya ejecución tarda mucho tiempo. Vea el estado del trabajo en la página **Trabajos y registros**.

Asignar e implementar

En OMIMSSC, haga clic en **Configuración e implementación** y, luego, en **Vista de servidor**. Seleccione los servidores en los que desea implementar una plantilla y, luego, haga clic en **Implementar Plantilla operativa**. Aparecerá el asistente **Implementar Plantilla operativa**.

Ejecutar actualización

1. En OMIMSSC, haga clic en **Centro de mantenimiento**, seleccione los servidores o grupos de sistema modular y una fuente de actualización; luego, haga clic en **Ejecutar actualización**.
2. Seleccione los servidores o grupos de sistema modular y un origen de actualización; luego, haga clic en **Ejecutar actualización**.
3. Ingrese un nombre único de trabajo y una descripción para el trabajo; luego, haga clic en **Crear**.

Para realizar un seguimiento de este trabajo, se selecciona la opción **Ir a la lista de trabajos** de forma predeterminada.

Implementar un clúster Azure Stack HCI

1. Cree los perfiles de credenciales del dispositivo y de Windows requeridos.
2. Cree una imagen de WinPE
 - a. Instale la función WDS en SCVMM y, a continuación, configúrela.
 - b. Agregue el servidor PXE en el servidor SCVMM mediante [agregar recursos](#) y especifique el mismo nombre de servidor (nombre de host SCVMM) y servidor PXE.
 - c. Cree la carpeta de recursos compartidos dentro del servidor SCVMM y, a continuación, copie Boot.wim desde C:\RemoteInstall\DCMgr\Boot\Windows\Images en una carpeta de recursos compartidos.
 - d. [Descargue Dell EMC OpenManage Deployment Toolkit](#) y extraiga el archivo en una carpeta de recursos compartidos creada. Por ejemplo, \\Servername\sharefolder\DTK\DTK501.
 - e. [Cree una imagen de WinPE](#).
 - f. Asegúrese de que la imagen de WinPE se coloque en una carpeta de recursos compartidos en SCVMM.
3. Agregue la plantilla de VM de Windows Server 2016 y 2019 a la biblioteca de SCVMM. Para obtener más información, consulte la [documentación de Microsoft](#).
 - a. Cambie las siguientes propiedades:
 - Sistema operativo: Windows Server 2016 y 2019 Datacenter
 - Plataforma de virtualización: Microsoft Hyper-V

 **NOTA:** Para crear un disco virtual de Windows Server 2019 (.vhdx) mediante el archivo .iso para la implementación del sistema operativo, consulte <https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f>
4. Cree un perfil de equipo físico (PCP) en SCVMM. En la configuración de hardware > disco y particiones, seleccione el esquema de partición como **Tabla de particiones GUID**. Para obtener más información, consulte [Crear un perfil de equipo físico](#) en la sección Requisitos previos de la documentación de Microsoft sobre el aprovisionamiento de un host o clúster de Hyper-V desde computadoras vacías.
5. Cree un grupo de hosts en SCVMM para alojar el clúster Azure Stack HCI. Para obtener información acerca de cómo crear grupos de hosts en SCVMM, consulte la documentación de Microsoft.
6. [Cree un perfil de hipervisor](#).
7. [Detecte los servidores en la extensión de Dell EMC OpenManage](#).
8. [Configure mediante la plantilla operativa predefinida](#).
9. (Opcional) Compruebe el cumplimiento (configuración e implementación > servidor > seleccionar el servidor y asignar una plantilla operativa).
10. [Cree un switch lógico](#).
11. [Implemente el clúster Azure Stack HCI](#).

Para verificar que la implementación del clúster se haya realizado correctamente, vaya a **Vista de clúster** para comprobar si el clúster aparece con la categoría correspondiente.

Escenarios de solución de problemas

Temas:

- Recursos necesarios para administrar OMIMSSC OMIMSSC
- Verificación de los permisos de uso de la extensión de la consola de OMIMSSC para SCCM
- Verificación de los permisos de PowerShell para usar la extensión de la consola de OMIMSSC para SCVMM
- Instalación y actualización de escenarios en OMIMSSC OMIMSSC
- OMIMSSC Escenarios de portal de administración de OMIMSSC
- Escenarios de descubrimiento, sincronización e inventario en OMIMSSC OMIMSSC
- Escenarios genéricos en OMIMSSC OMIMSSC
- Escenarios de actualización del firmware en OMIMSSC OMIMSSC
- Escenarios de implementación del sistema operativo en OMIMSSC
- Escenarios de perfil del servidor en OMIMSSC
- Escenarios de registros de LC en OMIMSSC

Recursos necesarios para administrar OMIMSSC OMIMSSC

Utilice esta guía para buscar los privilegios necesarios y resolver cualquier problema generado en OMIMSSC.

Para solucionar los problemas que se generan en OMIMSSC, asegúrese de tener los siguientes recursos:

- Detalles de la cuenta del usuario de solo lectura para iniciar sesión en el dispositivo OMIMSSC y realizar distintas operaciones.

Para iniciar sesión como usuario de solo lectura en la VM del dispositivo OMIMSSC, introduzca el nombre de usuario como `readOnly` con la misma contraseña utilizada para iniciar sesión en la VM del dispositivo OMIMSSC.

- Registre los archivos de alto nivel y complete los detalles sobre los errores:
 - Registros de actividades: contienen información específica del usuario y de alto nivel sobre los trabajos iniciados en OMIMSSC y el estado de los trabajos ejecutados en OMIMSSC. Para ver los registros de actividades, vaya a la página **Trabajos y registros** en la extensión de la consola de OMIMSSC.
 - Registros completos: contienen registros relacionados con los administradores y varios registros detallados específicos para escenarios de OMIMSSC. Para ver los registros completos, vaya a la página **Trabajos y registros** en el **Portal de administración de OMIMSSC, Configuración** y, a continuación, **Registros**.
 - Registros de LC: contienen información a nivel del servidor, es decir, mensajes de error detallados sobre las operaciones realizadas en OMIMSSC. Para descargar y visualizar los registros de LC, consulte la *Guía del usuario de OpenManage Integration de Microsoft System Center de Dell EMC para System Center Configuration Manager y System Center Virtual Machine Manager*.

NOTA: Para solucionar problemas en dispositivos individuales de iDRAC o de la página OpenManage Enterprise Module (OME-Modular), inicie OMIMSSC, haga clic en la página **Configuración e implementación**, inicie la vista correspondiente y, a continuación, haga clic en la URL de la dirección IP del dispositivo.

NOTA: La cuenta del usuario administrador de servidor de SCVMM no debe ser una cuenta de servicio de SCVMM.

NOTA: Si está actualizando de SC2012 VMM SP1 a SC2012 VMM R2, actualice a Windows PowerShell 4.0.

Verificación de los permisos de uso de la extensión de la consola de OMIMSSC para SCCM

Después de instalar OMIMSSC, verifique que el usuario inscrito tenga los siguientes permisos:

1. En el sistema en el que OMIMSSC está instalado, proporcione los permisos de **Escritura** para la carpeta `<Configuration Manager Admin Console Install Dir>\XmlStorage\Extensions\DLPlugin` con los comandos PowerShell.

Complete los siguientes requisitos previos en el servidor del sitio y en el servidor proveedor de SMS antes de instalar el componente de OMIMSSC:

- a. En PowerShell, ejecute el comando: `PSRemoting`.

Si se deshabilita el comando `PSRemoting`, habilite el comando `PSRemoting` con los siguientes comandos.

- i. Ejecute el comando `Enable-PSRemoting`.
- ii. En el mensaje de confirmación, escriba `Y`.

- b. En PowerShell, ejecute el comando: `Get-ExecutionPolicy`.

Si la política no se establece en `RemoteSigned`, seleccione `RemoteSigned` con los siguientes comandos.

- i. Ejecute el comando `Set-ExecutionPolicy RemoteSigned`.
- ii. En el mensaje de confirmación, escriba `Y`.

2. Configure el acceso del usuario a Windows Management Instrumentation (WMI). Para obtener más información, consulte [Configuración de acceso de usuario al Instrumental de administración de Windows \(WMI, por sus siglas en inglés\)](#).

3. Otorgue permisos de compartir y de carpeta para escribir archivos en la carpeta de bandeja de entrada.

Para otorgar permisos de compartir y de carpeta para escribir archivos en la bandeja de entrada de DDR:

- a. Desde la consola Configuration Manager, bajo **Administración**, otorgue al usuario permiso para escribir en el recurso compartido **SMS_<sitecode>**.

- b. Mediante el **Explorador de archivos**, vaya a la ubicación del recurso compartido **SMS_<sitecode>** y, a continuación, a la carpeta `ddm.box`. Otorgue control completo al usuario de dominio para las siguientes carpetas:

- **SMS_<sitecode>**
- Bandejas de entrada
- `ddm.box`

Configuración de acceso de usuario a WMI

Para configurar el acceso del usuario a WMI de manera remota:

 **NOTA:** Asegúrese de que el servidor de seguridad del sistema no bloquee la conexión WMI.

1. Para acceder al modelo de objeto de componente distribuido (DCOM, por sus siglas en inglés) de forma remota, proporcione los permisos para los usuarios inscritos en SCCM.

Para otorgar permisos de usuario para DCOM:

- a. Inicie `dcomcnfg.exe`

- b. En el panel izquierdo de la consola **Servicios de componentes**, amplíe **Computadoras**, haga clic con el botón secundario en **Mi computadora** y seleccione **Propiedades**.

- c. En **Seguridad de COM**:

- A partir de **Permisos de acceso**, haga clic en **Editar límites** y seleccione **Acceso remoto**.
- En **Inicio y permiso de activación**, haga clic en **Editar límites** y seleccione **Inicio local, Inicio remoto y Activación remota**.

2. Para acceder a los componentes de administración e instrumentación de Windows (WMI) para configurar DCOM, proporcione los permisos de usuario para los usuarios inscritos.

Para otorgar permisos de usuario para DCOM Config WMI:

- a. Inicie `dcomcnfg.exe`

- b. Amplíe **Mi computadora** > **Configuración de DCOM**.

- c. Haga clic con el botón derecho del mouse en **Administración e instrumentación de Windows** y seleccione **Propiedades**.

- d. En **Seguridad**, en **Inicio y permiso de activación**, haga clic en **Editar** y seleccione los permisos de **Inicio remoto y Activación remota**.
3. Configure la seguridad de un espacio de nombre y otorgue los permisos.
Para configurar la seguridad de espacio de nombre y otorgar permisos:
 - a. Inicie `wimgmt.msc`
 - b. En el panel **Control WMI**, haga clic con el botón secundario en **Control WMI**, seleccione **Propiedades** y, a continuación, seleccione **Seguridad**.
 - c. Vaya a `ROOT\SMS Namespace`.
 - d. Seleccione los permisos **Ejecutar métodos**, **Escritura del proveedor**, **Activar cuenta** y **Habilitación remota**.
 - e. Vaya a `Root\cimv2\OMIMSSC`.
 - f. Seleccione los permisos **Ejecutar métodos**, **Proporcionar escritura**, **Activar cuenta** y **Habilitación remota**.
Como alternativa, el usuario de Configuration Manager se convierte en miembro del grupo **SMS_Admin** y es posible agregar **Habilitación remota** a los permisos existentes del grupo.

Verificación de los permisos de PowerShell para usar la extensión de la consola de OMIMSSC para SCVMM

Compruebe si el estado **PSRemoting** está activado y **ExecutionPolicy** está configurado como **RemoteSigned**. Si el estado es diferente, realice los siguientes pasos en PowerShell:

- a. En PowerShell, ejecute el comando: `PSRemoting`.
Si se deshabilita el comando `PSRemoting`, habilite el comando `PSRemoting` con los siguientes comandos.
 - i. Ejecute el comando `Enable-PSRemoting`.
 - ii. En el mensaje de confirmación, escriba `Y`.
- b. En PowerShell, ejecute el comando: `Get-ExecutionPolicy`.
Si la política no se establece en `RemoteSigned`, seleccione `RemoteSigned` con los siguientes comandos.
 - i. Ejecute el comando `Set-ExecutionPolicy RemoteSigned`.
 - ii. En el mensaje de confirmación, escriba `Y`.

Instalación y actualización de escenarios en OMIMSSC

En esta sección, se muestra toda la información de solución de problemas relacionada con la instalación y actualización de OMIMSSC.

Verificación de la configuración de la máquina virtual (VM) del dispositivo OMIMSSC

Para verificar que la VM del dispositivo OMIMSSC se configure de manera adecuada, seleccione la opción VM del dispositivo OMIMSSC y luego haga clic con el botón secundario en ella. A continuación, haga clic en **Configuración** y realice las siguientes tareas:

1. Compruebe si la asignación de memoria para el dispositivo OMIMSSC cumple con el requisito que se menciona en la sección *Requisitos comunes* de la *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*. De lo contrario, ingrese la memoria en **RAM de inicio** y haga clic en **Aplicar**.
2. Compruebe si el recuento de procesadores cumple con el requisito que se menciona en la sección *Requisitos comunes* de la *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*. De lo contrario, proporcione la cantidad de conteos de procesadores en el conteo **Cantidad de procesadores virtuales** en **Procesadores**.
3. Verifique si aparece el campo **Disco duro virtual** en Controladora IDE: **Controladora IDE 0 > Disco duro** y si el campo **Disco duro virtual** aparece en el archivo **OMIMSSC—v7**. De lo contrario, haga clic en **Examinar**, vaya a la ubicación en la que se descomprimió el archivo VHD, seleccione el archivo **OMIMSSC—v7** y haga clic en **Aplicar**.

4. Verifique si el **Adaptador de red > Switch virtual** está conectado a una tarjeta NIC física. De lo contrario, configure la tarjeta NIC, seleccione la tarjeta NIC apropiada en el menú desplegable **Switch virtual** y haga clic en **Aplicar**.

Si la máquina virtual creada recientemente con el disco duro virtual seleccionado para el dispositivo OMIMSSC no arranca con alguna excepción de kernel panic, edite la configuración de la máquina virtual y active la opción de memoria dinámica para esta máquina virtual. Para activar la opción de memoria dinámica en la máquina virtual, realice las siguientes tareas:

1. Haga clic con el botón secundario en la VM del dispositivo OMIMSSC y haga clic en **Configuración**, y, a continuación, en **Memoria**.
2. En **Memoria dinámica**, seleccione la casilla de verificación **Habilitar memoria dinámica** e introduzca los detalles.

Falla en la inscripción

Si la conexión de prueba o la inscripción fallan, aparecerá un mensaje de error.

Para solucionar este problema, realice los pasos siguientes:

- Haga ping desde el dispositivo OMIMSSC hacia el nombre de dominio completamente calificado (FQDN, por sus siglas en inglés) del servidor de SCCM o SCVMM inscrito, mediante el inicio de sesión en la VM del dispositivo OMIMSSC como usuario de solo lectura. Si hay una respuesta, espere un momento y continúe con la inscripción.

Para iniciar la VM del dispositivo OMIMSSC como usuario de solo lectura, introduzca el nombre de usuario como `readonly` con la misma contraseña que usó para iniciar sesión en la VM del dispositivo OMIMSSC.

- Asegúrese de que los servidores SCCM o SCVMM se estén ejecutando.
- La cuenta de Microsoft utilizada para inscribir la consola debe ser la de un administrador delegado o un administrador en System Center, y una de administrador local en el servidor de System Center.
- Específico para los usuarios de SCVMM:
 - Asegúrese de que el servidor de SCVMM no esté registrado en otro dispositivo OMIMSSC. Si desea registrar el mismo servidor de SCVMM en el dispositivo OMIMSSC, elimine el perfil de aplicación del **perfil de registro de OMIMSSC** desde el servidor de SCVMM.
 - Si aplicó una actualización de paquete acumulativo de SCVMM, seleccione el número del puerto TCP de Indigo de la consola de SCVMM en el registro (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings`). Utilice el mismo número de puerto que se utilizó para registrar consola de SCVMM. El número predeterminado es 8100.

Falla en la conexión de prueba

Si los nombres de usuario son idénticos y las contraseñas son diferentes en el caso de la cuenta de usuario de dominio y la cuenta de usuario local, se produce un error en la conexión de prueba entre la consola de Microsoft y el dispositivo OMIMSSC.

Por ejemplo, la cuenta de usuario de dominio es: `domain\user1` y la contraseña es `pwd1`. La cuenta de usuario local es `user1` y la contraseña es `Pwd2`. Cuando intenta inscribirse con la cuenta de usuario de dominio mencionada anteriormente, se produce un error en la conexión de prueba.

Como solución alternativa, utilice nombres de usuario distintos para el usuario de dominio y las cuentas de usuario local, o bien utilice una cuenta de usuario única como usuario local durante la inscripción de la consola de Microsoft en el dispositivo OMIMSSC.

Falla en la conexión de la extensión de la consola de OMIMSSC para SCVMM

Después de inscribir e instalar la extensión de la consola de OMIMSSC en un ambiente de SCVMM, cuando intenta iniciar OMIMSSC, se muestra el siguiente mensaje de error: `Connection to server failed`.

Para solucionar este problema, realice los pasos siguientes:

1. Cuando inicie OMIMSSC, agregue la dirección IP y el FQDN del dispositivo OMIMSSC a la intranet local en la consola de SCVMM.
2. Agregue la dirección IP y el FQDN del dispositivo OMIMSSC en **Zonas de búsqueda directa** y **Zonas de búsqueda inversa** en DNS.
3. Para obtener más detalles, compruebe si existen mensajes de error en el archivo `C:\ProgramData\VMMLogs\AdminConsole`.

Error en el acceso a la extensión de la consola después de actualizar SCVMM R2

Después de aplicar el paquete acumulativo de actualizaciones para VMM SC2012 R2, si intenta abrir la consola de OMIMSSC recientemente instalada, SCVMM muestra un mensaje de error por motivos de seguridad y no podrá acceder a la consola de OMIMSSC.

Para solucionar este problema, realice lo siguiente:

1. Elimine la carpeta en la ruta de acceso predeterminada: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\.`
2. Reinicie SCVMM.
3. Quite la extensión de la consola y, a continuación, impórtela como se indica en la sección *Importación de la extensión de la consola de OMIMSSC para SCVMM* de la *Guía de instalación de OpenManage Integration de Microsoft System Center de Dell EMC para System Center Configuration Manager y System Center Virtual Machine Manager*.

La dirección IP no está asignada al dispositivo OMIMSSC

Después de crear e iniciar la VM del dispositivo OMIMSSC, no se asigna o muestra la dirección IP del dispositivo OMIMSSC.

Como solución alternativa, compruebe si el switch virtual está asignado a un switch físico, si el switch está configurado correctamente y, a continuación, conéctese al dispositivo OMIMSSC.

SCVMM se bloquea durante la importación de la extensión de la consola de OMIMSSC

Es posible que la consola de administrador RTM VMM SC2016 compilación 4.0.1662.0 se bloquee durante la importación de la extensión de la consola de OMIMSSC.

Como solución alternativa, actualice SCVMM con el artículo KB 4094925 disponible en support.microsoft.com/kb/4094925 y, a continuación, importe la extensión de la consola de OMIMSSC.

Falla en el inicio de sesión en las extensiones de la consola de OMIMSSC

Después de iniciar sesión en las extensiones de la consola de OMIMSSC con diferentes credenciales para iniciar sesión en la consola de Microsoft, el inicio de sesión falla con el siguiente mensaje de error: `Username or Password is incorrect`.

Como solución alternativa, inicie la consola de Microsoft, e inicie sesión en ella, con las credenciales utilizadas para iniciar sesión en la extensión de la consola de OMIMSSC. Esta es una actividad que se puede realizar una vez.

Bloqueo de SC2012 VMM SP1 durante la actualización

Después de actualizar a SC2012 VMM SP1, la consola de SCVMM puede bloquearse cuando importe la extensión de la consola de OMIMSSC a SC2012 VMM UR5 o versiones posteriores.

Para obtener información sobre este problema y cómo solucionarlo, consulte el problema cinco en la dirección URL de esta base de conocimientos: support.microsoft.com/kb/2785682.

Como solución alternativa, actualice SCVMM independientemente de la versión del paquete acumulativo de actualizaciones instalado.

OMIMSSC Escenarios de portal de administración de OMIMSSC

En esta sección, se muestra toda la información de solución de problemas relacionada con el portal de administración de OMIMSSC.

Mensaje de error cuando se accede al portal de administración de OMIMSSC con el navegador Mozilla Firefox

Cuando accede al portal de administración de OMIMSSC con el navegador Mozilla Firefox, aparece el siguiente mensaje de advertencia: "Secure Connection Failed".

Para solucionar este problema, elimine el certificado creado a partir de una entrada anterior de el portal de administración en el navegador. Para obtener información sobre la eliminación del certificado del navegador Mozilla Firefox, consulte support.mozilla.org.

Falla en la muestra del logotipo de Dell EMC en la pantalla del portal de administración de OMIMSSC

Cuando se inicia el portal de administración de OMIMSSC en un navegador Internet Explorer predeterminado con Windows 2016, el portal de administración 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, a continuación, agregue la dirección URL del portal de administración de OMIMSSC a la lista de favoritos del navegador.

Escenarios de descubrimiento, sincronización e inventario en OMIMSSC OMIMSSC

En esta sección, se proporciona toda la información de solución de problemas de credenciales, servidores de descubrimiento, servidores de agrupación y sincronización de consolas inscritas de Microsoft en OMIMSSC cuando se utiliza OMIMSSC.

Falla en el descubrimiento de servidores

Cuando hay varias consolas de Microsoft inscritas en un dispositivo OMIMSSC y usted intenta descubrir un servidor, el trabajo de descubrimiento del servidor fallará si no se puede acceder a una de las consolas de SCCM.

Como solución alternativa, cancele la inscripción de la consola de SCCM a la que no se puede acceder, o bien solucione los errores y asegúrese de que se pueda acceder a la consola de SCCM desde el dispositivo OMIMSSC.

No se agregaron servidores descubiertos a toda la colección de All Dell Lifecycle Controller Servers

Después de descubrir servidores en OMIMSSC para la extensión de la consola de SCCM, es posible que el servidor no se agregue a la colección de **All Dell Lifecycle Controller Servers**.

Como solución alternativa, elimine la colección **All Dell Lifecycle Controller Servers** y, a continuación, descubra el servidor. La colección se crea automáticamente en SCCM y se agrega el servidor a este grupo.

Falla en el descubrimiento de servidores debido a credenciales incorrectas

Si proporciona detalles de credenciales incorrectos durante el descubrimiento, en función de la versión de iDRAC, están disponibles las siguientes resoluciones:

- ○ Cuando se descubre un servidor PowerEdge de 12.^a generación con la versión de iDRAC 2.10.10.10 o versiones posteriores, si se proporcionan detalles incorrectos del perfil de credenciales, fallará el descubrimiento del servidor y se mostrará 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 los detalles correctos del perfil de credenciales cuando se desbloquea la dirección IP.
- Si cambió el perfil de credencial predeterminado de iDRAC luego de descubrir y agregar un dispositivo, no se pueden realizar actividades en el servidor. Para trabajar en el servidor, vuelva a descubrir el servidor con el nuevo perfil de credencial.

Creación del grupo de chasis VRTX incorrecto después del descubrimiento de servidores

Cuando los servidores modulares que antes estaban en otro chasis se agregan a un chasis VRTX y se descubren en OMIMSSC, los servidores modulares llevan la información de la etiqueta de servicio del chasis anterior. Por lo tanto, se crea un grupo de chasis VRTX con información del chasis antiguo en el dispositivo, en lugar de tener la información más reciente sobre el chasis.

Para solucionar este problema, realice lo siguiente:

1. Habilite 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.

No se puede sincronizar los servidores host con SCCM inscrito

Durante la sincronización de la extensión de la consola de OMIMSSC con SCCM inscrito, los servidores no se muestran como subtareas en el trabajo de sincronización y, por lo tanto, no se sincronizan.

Como solución alternativa, inicie la consola de SCCM con “Ejecutar con privilegios de administrador” y actualice la configuración fuera de banda para un servidor. Luego, sincronice la extensión de la consola de OMIMSSC con SCCM inscrito.

Para obtener más información, consulte el tema Sincronizar con consolas Microsoft inscritas en la *Guía del usuario de OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*.

No se elimina el grupo de actualización de clúster vacío durante el descubrimiento automático o la sincronización

Cuando se descubre un clúster en OMIMSSC, se crea un grupo de actualización de clúster en el **Centro de mantenimiento** con todos los servidores incluidos en este grupo. Después de esto, si se quitan todos los servidores de este clúster a través de SCVMM, y se realiza un descubrimiento automático o una sincronización con la operación SCVMM, no se elimina el grupo de actualización de clúster vacío en el **Centro de mantenimiento**.

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

Falla en la realización de tareas relacionadas con el mantenimiento en los servidores que se volvieron a descubrir

Cuando elimina un servidor o todos los servidores de un grupo de actualización de OMIMSSC y vuelve a descubrirlos, no se pueden realizar otras operaciones en estos servidores, como actualizar el firmware, exportar e importar registros de LC, y exportar e importar perfiles del servidor.

Como solución alternativa, después de volver a descubrir el o los servidores eliminados, realice actualizaciones del firmware mediante la función **Implementar plantilla operacional** en **Vista del servidor** y, para otros escenarios de mantenimiento, utilice iDRAC.

Escenarios genéricos en OMIMSSC OMIMSSC

Esta sección contiene información de solución de problemas que es independiente de cualquier flujo de trabajo en OMIMSSC.

Falla en el acceso al recurso compartido CIFS con hostname

Los servidores modulares no pueden acceder al recurso compartido CIFS mediante el uso del hostname para realizar cualquier trabajo en OMIMSSC.

Como solución alternativa, especifique la dirección IP del servidor que tiene el recurso compartido CIFS en lugar del hostname.

Falla en la muestra de la página de trabajos y registros en la extensión de la consola

La página **Centro de trabajos y registros** no aparece en la extensión de la consola de OMIMSSC.

Como solución alternativa, vuelva a inscribir la consola y, a continuación, inicie la página **Trabajos y registros**.

Falla de las operaciones en los sistemas administrados

Todas las funciones de OMIMSSC no se realizan del modo esperado en los sistemas administrados debido a una versión de Transport Layer Security (TLS).

Si utiliza versión de firmware del iDRAC 2.40.40.40 o posterior, la opción Seguridad de la capa de transporte (TLS) está activada de forma predeterminada en las versiones 1.1 o posterior. Antes de instalar la extensión de la consola, instale la actualización para habilitar TLS 1.1 y versiones posteriores, como se indica en el siguiente artículo de KB: support.microsoft.com/en-us/kb/3140245. Se recomienda habilitar la compatibilidad con TLS 1.1 o versiones posteriores en su servidor y consola de SCVMM para asegurarse de que OMIMSSC funcione como se espera. Para obtener más información sobre iDRAC, consulte Dell.com/idracmanuals.

Falla en el inicio de la ayuda en línea para OMIMSSC

Cuando utiliza el sistema operativo Windows 2012 R2, se inicia el contenido de ayuda en línea relativa al contexto con un mensaje de error.

Como solución, actualice el sistema operativo con los artículos de la base de conocimientos (KB) más recientes y, a continuación, vea el contenido de ayuda en línea.

Escenarios de actualización del firmware en OMIMSSC OMIMSSC

En esta sección, se presenta toda la información de solución de problemas de orígenes de actualización, grupos de actualización, repositorios e inventario después de las actualizaciones.

Error de creación de origen de actualización

Cuando se cambia la configuración de red del sistema de nombres de dominio (DNS, por sus siglas en inglés) del dispositivo, falla la creación del tipo HTTP o FTP del origen de actualización.

Como solución alternativa, reinicie el dispositivo y, a continuación, cree el origen de actualización de tipo HTTP o FTP.

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

Después de instalar y configurar, actualizar o migrar OMIMSSC, cuando intente acceder al sitio FTP con un **catálogo en línea de Dell** de origen de actualización predeterminado, podría fallar si se necesitan credenciales de proxy.

Como solución alternativa, para acceder al sitio FTP con el **catálogo en línea de Dell** como origen de actualizaciones, edite el origen de actualizaciones para agregar las credenciales de proxy.

Falla en la conexión de prueba del origen local de actualizaciones

Después de proporcionar los detalles de un origen local de actualizaciones, la conexión de prueba puede fallar, ya que es posible que no se pueda acceder a los archivos necesarios.

Como solución alternativa, asegúrese de que el archivo `catalog.gz` se encuentre en la siguiente estructura de carpetas.

- En el caso del origen de actualizaciones para HTTP local: `http:\\IP address\catalog\catalog.gz`
- En el caso del origen de actualizaciones para FTP local: `ftp:\\IP address\catalog\catalog.gz`
- En el caso del origen de actualizaciones para DRM local: `\\IP address\catalog\<catalogfile>.gz`

Falla en la creación de un origen de actualización de DRM

Es posible que falle la creación de una fuente de actualización de DRM en el servidor de administración que se ejecuta en el sistema operativo (SO) Windows 10, y se muestre el siguiente mensaje de error: `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Consulte el registro **omimsscappliance_main** en el portal de administración de OMIMSSC si el mensaje de error que se muestra es el siguiente: `Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`

Como solución alternativa, consulte el siguiente artículo de KB: support.microsoft.com/en-us/help/4034314.

Falla en la creación de un repositorio durante una actualización del firmware

La creación de un repositorio puede fallar durante una actualización del firmware debido a que se proporcionaron las credenciales incorrectas durante la creación de un origen de actualización, o bien no se puede acceder al origen de actualización del dispositivo OMIMSSC.

Como solución alternativa, asegúrese de que se pueda acceder al origen de la actualización desde la ubicación en la que se aloja el dispositivo OMIMSSC y proporcione las credenciales correctas durante la creación de un origen de actualización.

Error en la muestra del informe de comparación después de actualizar o migrar OMIMSSC

Después de actualizar a la versión más reciente de OMIMSSC, si falla la conexión a `ftp.dell.com` o `downloads.dell.com`, el FTP en línea predeterminado de Dell o el origen de actualización HTTP de Dell no podrán descargar el archivo del catálogo. Por lo tanto, el informe de comparación no se encuentra disponible.

Como solución alternativa, a fin de ver un informe de comparación para el origen de actualización predeterminado, edite el FTP en línea predeterminado de Dell o el origen de actualización HTTP de Dell, cree credenciales de proxy y, a continuación, seleccione el origen de actualización desde el menú desplegable **Seleccionar origen de actualización**. Para obtener más información sobre cómo editar un origen de actualización, consulte la sección *Modificación del origen de actualización* en la *Guía del usuario de OpenManage Integration de Microsoft System Center de Dell EMC para System Center Configuration Manager y System Center Virtual Machine Manager*.

Falla en la actualización del firmware de los clústeres

Después del envío de un trabajo a OMIMSSC para actualizar el firmware de los clústeres, estos no se actualizan debido a ciertas causas que aparecen en los siguientes mensajes de error en los **registros de actividades**.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

NOTA: Las acciones de actualización compatibles con clústeres se registran en las siguientes ubicaciones: \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports folder en la que se almacenará el informe de actualización compatible con clústeres. La carpeta \\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log folder contendrá los registros del plug-in de Dell EMC System Update (DSU) para cada nodo. Los registros del script extendido están disponibles en la ubicación de `C:\Window\Temp`, que consta de los archivos `precau.log` y `postcau.log` en cada nodo del clúster para el clúster S2D.

Causas de la falla en la actualización del firmware en los clústeres con la siguiente solución alternativa:

- Si los paquetes de actualización de Dell (DUP, por sus siglas en inglés) y los archivos de catálogos necesarios no están presentes en el origen de actualización local seleccionado.

Como solución alternativa, asegúrese de que todos los DUP y los archivos de catálogos estén disponibles en el repositorio y, a continuación, actualice el firmware de los clústeres.

- El grupo de clústeres deja de responder o se canceló el trabajo de actualización del firmware en la actualización compatible con clústeres (CAU, por sus siglas en inglés) debido a un trabajo en progreso; los DUP se descargan y se ubican en cada nodo del clúster de los servidores que pertenecen al grupo de clústeres.

Como solución alternativa, elimine todos los archivos de la carpeta Dell y, a continuación, actualice el firmware de los clústeres.

- Si Lifecycle Controller (LC) está ocupado con otras operaciones, la tarea de actualización del firmware en un nodo del clúster fallará. Para comprobar si la actualización falló debido a que LC está ocupado, busque el siguiente mensaje de error en cada nodo del clúster en la siguiente ruta: `C:\dell\suu\invcolError.log`.

```
Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then reboot the system.
```

Como solución alternativa, apague el servidor, quite los cables de alimentación y reinicie el servidor. Después del reinicio, actualice el firmware de los clústeres.

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

El trabajo de actualización del firmware enviado desde OMIMSSC a iDRAC falla y en el registro principal de OMIMSSC se muestra el siguiente error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s)`.

Como solución alternativa, elimine manualmente los trabajos terminados en iDRAC y reintente el trabajo de actualización del firmware. Para obtener más información sobre la eliminación de trabajos en iDRAC, consulte la documentación de iDRAC en dell.com/support/home.

Falla en la actualización del firmware con un origen de actualización de DRM

Es posible que el trabajo de actualización del firmware falle si utiliza un origen de actualización de DRM con acceso insuficiente a las carpetas compartidas. Si el perfil de credencial de Windows proporcionado cuando se creó el origen de actualización de DRM no forma parte del grupo de administradores de dominio o del grupo de administradores locales, se mostrará el siguiente mensaje de error: `Local cache creation failure`.

Como solución alternativa, realice los siguientes pasos:

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 **Seguridad** y, a continuación, haga clic en la pestaña **Avanzada**.
2. Haga clic en **Habilitar herencia** y seleccione la opción **Sustituir todas las entradas con permisos de objetos secundarios con entradas de permisos heredables de este objeto** y, a continuación, comparta la carpeta con **Todos** con permiso de lectura y escritura.

Actualización del firmware en componentes independientemente de la selección

Los mismos componentes en servidores idénticos se actualizan durante una actualización del firmware, independientemente de la selección de los componentes en estos servidores individuales. Este comportamiento se observa en los servidores PowerEdge de 12.^a y 13.^a generaciones con licencia de iDRAC Enterprise.

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

- Primero, aplique las actualizaciones para los componentes comunes en los servidores idénticos y, a continuación, aplique actualizaciones para los componentes específicos en los servidores individuales.
- Realice las actualizaciones en etapas con tiempos de interrupción planificados para realizar la actualización del firmware.

Falla en la muestra de información de inventario más reciente después de actualizar el firmware

Después de actualizar correctamente las versiones del firmware de los servidores PowerEdge de 11.^a generación, no se muestra la información de inventario más reciente.

En OMIMSSC, la actualización del inventario es una actividad que se realiza inmediatamente después de completar un trabajo de actualización del 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.

Como solución alternativa, verifique si se terminó la actividad de Collect System Inventory On Reboot (CSIOR) en el servidor PowerEdge y, a continuación, actualice el inventario del firmware en OMIMSSC. Además, asegúrese de reiniciar el servidor después de aplicar la actualización preconfigurada sin agente. Para obtener más información sobre la actualización del inventario, consulte la sección *Visualización y actualización del inventario del firmware* en la *Guía del usuario de OpenManage Integration para Microsoft System Center Configuration Manager y System Center Virtual Machine Manager*.

Para obtener más información sobre CSIOR, consulte la sección Solución de problemas en la versión más reciente de la *Guía del usuario de la interfaz gráfica de usuario (GUI, por sus siglas en inglés) de Dell Lifecycle Controller* disponible en dell.com/support/home.

Error al eliminar un grupo de actualización personalizado

Después de programar cualquier trabajo en un servidor perteneciente a un grupo personalizado de actualizaciones, si se elimina el servidor de la consola de Microsoft y se sincroniza la consola registrada de Microsoft con OMIMSSC, se quita el servidor del grupo personalizado de actualizaciones y se transfiere a un grupo predeterminado de actualizaciones. No puede eliminar este grupo personalizado de actualizaciones, debido a que se asocia a un trabajo programado.

Como solución alternativa, elimine el trabajo programado en la página **Trabajos y registros** y, a continuación, elimine el grupo personalizado de actualizaciones.

Falla en la actualización de la imagen de WinPE

Cuando intenta actualizar la imagen de WinPE, el trabajo de actualización puede fallar y se muestra el siguiente mensaje de error: `Remote connection to console failed.`

Como solución alternativa, ejecute el comando **DISM** para limpiar todas las imágenes anteriormente montadas en la consola de Microsoft y, a continuación, reintente actualizar la imagen de WinPE.

Cambio del color de la campana para el sondeo y la notificación después de actualizar la frecuencia

Si no se descubrió un servidor administrado en OMIMSSC y usted cambia la frecuencia de la opción de sondeo y notificación, el color de la campana cambiará a amarillo después de unos minutos, incluso si no hay cambios en el catálogo.

Como solución alternativa, descubra los servidores administrados y, a continuación, cambie la frecuencia de la opción de sondeo y de notificación.

Escenarios de implementación del sistema operativo en OMIMSSC

En esta sección, se proporciona toda la información de solución de problemas del sistema operativo o la implementación del hipervisor (para SCVMM) con una Plantilla operacional en OMIMSSC.

Escenarios genéricos de implementación del sistema operativo

En esta sección, se proporciona toda la información general de solución de problemas relacionada con la implementación del sistema operativo.

Falla en la implementación de una Plantilla operacional

Después de implementar la Plantilla operacional en los servidores seleccionados, los atributos o los valores de atributos no son apropiados para el archivo .CSV seleccionado, o se cambia la dirección IP o las credenciales de iDRAC debido a la configuración de la plantilla. El trabajo en iDRAC se realiza correctamente; sin embargo, el estado de este trabajo en OMIMSSC aparece como incorrecto o con fallas debido al archivo .CSV no válido, o bien no se pudo realizar un seguimiento del trabajo debido a los cambios de iDRAC en el servidor de destino.

Como solución alternativa, asegúrese de que el archivo .CSV seleccionado tenga todos los atributos y valores de atributos adecuados, y que la dirección IP o las credenciales de iDRAC no cambien debido a la configuración de la plantilla.

Falla al guardar una Plantilla operacional

Cuando cree una Plantilla operacional, si selecciona y borra la casilla de verificación de un atributo dependiente con un valor pool, no podrá guardar la plantilla operacional con el siguiente mensaje de error:

```
Select atleast one attribte, under the selected components, before creating the Operational Template.
```

Como solución alternativa, realice una de las siguientes acciones:

- Seleccione cualquier otro atributo dependiente con un valor de pool, o bien el mismo atributo dependiente, y guarde la plantilla operacional.
- Cree una nueva plantilla operacional.

Escenarios de implementación del sistema operativo para los usuarios de SCCM

En esta sección, se proporciona toda la información de solución de problemas relacionada con la implementación de sistemas operativos mediante OMIMSSC en la consola de SCCM.

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

La opción **Implementar** no se muestra en una secuencia de tareas existente después de desinstalar y reinstalar la extensión de la consola de OMIMSSC para SCCM.

Como solución alternativa, abra la secuencia de tareas para editarla, vuelva a habilitar la opción **Aplicar** y haga clic en **Aceptar**. Se muestra nuevamente la opción **Implementar**.

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

1. Haga clic con el botón secundario 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 **Aceptar**.

Esto reactiva la opción **Aplicar**.

Falla en la agregación de servidores en la colección Managed Lifecycle Controller Lifecycle Controller ESXi en SCCM

Si la búsqueda de DHCP falla durante la implementación del sistema operativo, el servidor agota el tiempo de espera y no se transfiere a la colección Managed Lifecycle Controller Lifecycle Controller (ESXi) en SCCM.

Como solución alternativa, instale el servidor de cliente de SCCM y, a continuación, realice una sincronización para agregar los servidores a la colección Managed Lifecycle Controller Lifecycle Controller (ESXi).

Escenarios de implementación del sistema operativo para los usuarios de SCVMM

En esta sección, se proporciona toda la información de solución de problemas relacionada con la implementación de hipervisores mediante OMIMSSC en la consola de SCVMM.

Falla en la implementación de hipervisores debido a LC o la protección del firewall

La implementación del hipervisor falla y se muestra el siguiente mensaje de error en el registro de actividades: `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 una 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 firewall pueden restringir la ejecución correcta del comando `WINRM`.

Consulte el siguiente artículo de KB como solución alternativa: 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 se muestra el siguiente mensaje de error en el registro de actividades:

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

Estos problemas pueden ocurrir debido a una salida de excepción 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:

1. En la consola de SCVMM, seleccione **Biblioteca > Servidores de biblioteca** y, a continuación, seleccione el servidor de la puerta de enlace de integración (IG, por sus siglas en inglés) que se agregó como servidor de 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.

Después de esto, puede implementar los hipervisores.

Error 21119 de SCVMM cuando se agregan servidores a Active Directory

Cuando se agregan 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 computer was expected to join Active Directory using the computer name <host.domain>.`

Para solucionar este problema, realice lo siguiente:

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. Después de agregar el servidor a SCVMM, vuelva a descubrirlo en OMIMSSC.

Ahora el servidor aparece en la pestaña **Host**.

Falla en la instalación del controlador de Lifecycle Controller (LC)

Cuando implementa un sistema operativo e instala controladores de LC con VMM SC2012, el sistema operativo se implementa correctamente, pero no se instalan los controladores de LC.

Para resolver el problema, aplique el paquete acumulativo más reciente de SCVMM.

Escenarios de creación de clústeres S2D para usuarios de SCVMM

En esta sección, se proporciona toda la información de solución de problemas relacionada con la creación de Storage Spaces Direct con OMIMSSC en la consola de SCVMM.

El estado de la condición del clúster S2D es desconocido

Cuando crea un clúster de Storage Spaces Direct en los nodos que formaban parte de un clúster existente, el pool de almacenamiento y la configuración de disco tienen la configuración del clúster existente. Por lo tanto, es posible que no se cree el pool de almacenamiento del clúster y, si se crea, el estado de la condición puede aparecer como desconocido.

Como solución alternativa, borre el pool de almacenamiento y la configuración de disco que tienen detalles del clúster existente y, a continuación, cree el clúster de Storage Spaces Direct. Para obtener más información sobre cómo borrar el pool de

almacenamiento, consulte la sección *Solución de problemas de los estados operativos y de condición de Storage Spaces Direct* en la documentación de Microsoft.

Escenarios de perfil del servidor en OMIMSSC

En esta sección, se muestra toda la información de solución de problemas de exportación e importación de perfiles de servidores en OMIMSSC.

Error al exportar perfiles de servidores

Después de programar un trabajo de exportación de perfil de servidor, el perfil de servidor no se exporta y aparece el siguiente mensaje de error: `The selectors for the resource are not valid.`

Como solución alternativa, restablezca iDRAC y, a continuación, programe el trabajo de exportación del perfil del servidor. Para obtener más información, consulte la documentación sobre iDRAC disponible en dell.com/support.

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

Después de enviar el trabajo de importación de perfil de servidor a OMIMSSC, se agotará el tiempo de espera del trabajo pasadas dos horas.

Para solucionar este problema, realice los pasos siguientes:

1. Inicie el servidor, presione F2 y, a continuación, introduzca la **Configuración del BIOS**.
2. Haga clic en **Configuración del sistema** y seleccione **Otros ajustes**.
3. Deshabilite **Indicador de F1/F2 en caso de error**.

Después de realizar los siguientes pasos, exporte nuevamente el perfil del servidor y utilice el mismo perfil del servidor para importar hacia ese servidor.

Escenarios de registros de LC en OMIMSSC

En esta sección, se muestra toda la información de solución de problemas relacionada con la exportación y visualización de los registros LC.

Falla en la exportación de registros de LC en formato .CSV

Cuando intenta descargar los archivos de registro de LC en formato .CSV, falla la operación de descarga.

Como solución alternativa, agregue el FQDN del dispositivo OMIMSSC en el navegador del sitio de intranet local. Para obtener más información sobre cómo agregar el dispositivo OMIMSSC en la intranet local, consulte la sección *Visualización de registros de LC* en la *Guía del usuario de Dell EMC OpenManage Integration para Microsoft System Center versión 7.2.1 para System Center Configuration Manager y System Center Virtual Machine Manager*.

Falla en la apertura de los archivos de registro de LC

Después de recopilar los registros de LC, cuando intente ver los archivos 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"`.

Como solución alternativa, restablezca el iDRAC y, a continuación, recopile y vea los registros de LC. Para obtener más información sobre el restablecimiento de iDRAC, consulte la documentación de iDRAC disponible en dell.com/support.

Falla en la conexión de prueba

Si los nombres de usuario son idénticos y las contraseñas son diferentes en el caso de la cuenta de usuario de dominio y la cuenta de usuario local, se produce un error en la conexión de prueba entre la consola de Microsoft y el dispositivo OMIMSSC.

Por ejemplo, la cuenta de usuario de dominio es: `domain\user1` y la contraseña es `pwd1`. La cuenta de usuario local es `user1` y la contraseña es `Pwd2`. Cuando intenta inscribirse con la cuenta de usuario de dominio mencionada anteriormente, se produce un error en la conexión de prueba.

Como solución alternativa, utilice nombres de usuario distintos para el usuario de dominio y las cuentas de usuario local, o bien utilice una cuenta de usuario única como usuario local durante la inscripción de la consola de Microsoft en el dispositivo OMIMSSC.

Apéndice

Ingrese manualmente los valores de atributo de zona horaria en los dispositivos MX7000 consultando la tabla a continuación:

Tabla 12. Detalles de zona horaria

ID de zona horaria	Diferencia de zona horaria
TZ_ID_1	(GMT-12:00) Línea de fecha internacional, Oeste
TZ_ID_2	(GMT+14:00) Samoa
TZ_ID_3	(GMT-10:00) Hawái
TZ_ID_4	(GMT-09:00) Alaska
TZ_ID_5	(GMT-08:00) Hora del Pacífico (EE. UU. y Canadá)
TZ_ID_6	(GMT-08:00) Baja California
TZ_ID_7	(GMT-07:00) Arizona
TZ_ID_8	(GMT-07:00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07:00) Hora de las montañas (EE. UU. y Canadá)
TZ_ID_10	(GMT-06:00) América central
TZ_ID_11	(GMT-06:00) Hora central (EE. UU. y Canadá)
TZ_ID_12	(GMT-06:00) Guadalajara, Ciudad de México, Monterrey
TZ_ID_13	(GMT-06:00) Saskatchewan
TZ_ID_14	(GMT-05:00) Bogotá, Lima, Quito
TZ_ID_15	(GMT-05:00) Hora del Este (EE. UU. y Canadá)
TZ_ID_16	(GMT-05:00) Indiana (Este)
TZ_ID_17	(GMT-04:30) Caracas
TZ_ID_18	(GMT-04:00) Asunción
TZ_ID_19	(GMT-04:00) Hora del Atlántico (Canadá)
TZ_ID_20	(GMT-04:00) Cuiabá
TZ_ID_21	(GMT-04:00) Georgetown, La Paz, Manaos, San Juan
TZ_ID_22	(GMT-04:00) Santiago
TZ_ID_23	(GMT-03:30) Terranova
TZ_ID_24	(GMT-03:00) Brasilia
TZ_ID_25	(GMT-03:00) Buenos Aires
TZ_ID_26	(GMT-03:00) Cayena, Fortaleza
TZ_ID_27	(GMT-03:00) Groenlandia
TZ_ID_28	(GMT-03:00) Montevideo
TZ_ID_29	(GMT-02:00) Atlántico Medio
TZ_ID_30	(GMT-01:00) Azores
TZ_ID_31	(GMT-01:00) Islas de Cabo Verde

Tabla 12. Detalles de zona horaria (continuación)

ID de zona horaria	Diferencia de zona horaria
TZ_ID_32	(GMT+00:00) Casablanca
TZ_ID_33	(GMT+00:00) Tiempo universal coordinado
TZ_ID_34	(GMT+00:00) Dublín, Edimburgo, Lisboa, Londres
TZ_ID_35	(GMT+00:00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01:00) Ámsterdam, Berlín, Berna, Roma, Estocolmo, Viena
TZ_ID_37	(GMT+01:00) Belgrado, Bratislava, Budapest, Ljubljana, Praga
TZ_ID_38	(GMT+01:00) Bruselas, Copenhague, Madrid, París
TZ_ID_39	(GMT+01:00) Sarajevo, Skopje, Varsovia, Zagreb
TZ_ID_40	(GMT+01:00) África Central y Occidental
TZ_ID_41	(GMT+02:00) Windhoek
TZ_ID_42	(GMT+02:00) Amán
TZ_ID_43	(GMT+03:00) Estambul
TZ_ID_44	(GMT+02:00) Beirut
TZ_ID_45	(GMT+02:00) El Cairo
TZ_ID_46	(GMT+02:00) Damasco
TZ_ID_47	(GMT+02:00) Harare, Pretoria
TZ_ID_48	(GMT+02:00) Helsinki, Kiev, Riga, Sofía, Tallin, Vilnius
TZ_ID_49	(GMT+02:00) Jerusalén
TZ_ID_50	(GMT+02:00) Minsk
TZ_ID_51	(GMT+03:00) Bagdad
TZ_ID_52	(GMT+03:00) Kuwait, Riad
TZ_ID_53	(GMT+03:00) Moscú, San Petersburgo, Volgogrado
TZ_ID_54	(GMT+03:00) Nairobi
TZ_ID_55	(GMT+03:30) Teherán
TZ_ID_56	(GMT+04:00) Abu Dabi, Mascate
TZ_ID_57	(GMT+04:00) Bakú
TZ_ID_58	(GMT+04:00) Port Louis
TZ_ID_59	(GMT+04:00) Tiflis
TZ_ID_60	(GMT+04:00) Ereván
TZ_ID_61	(GMT+04:30) Kabul
TZ_ID_62	(GMT+05:00) Ekaterimburgo
TZ_ID_63	(GMT+05:00) Islamabad, Karachi
TZ_ID_64	(GMT+05:00) Taskent
TZ_ID_65	(GMT+05:30) Madrás, Calcuta, Bombay, Nueva Delhi
TZ_ID_66	(GMT+05:30) Sri Jayawardenepura
TZ_ID_67	(GMT+05:45) Katmandú
TZ_ID_68	(GMT+06:00) Astaná

Tabla 12. Detalles de zona horaria (continuación)

ID de zona horaria	Diferencia de zona horaria
TZ_ID_69	(GMT+06:00) Daca
TZ_ID_70	(GMT+06:00) Novosibirsk
TZ_ID_71	(GMT+06:30) Yangón (Rangún)
TZ_ID_72	(GMT+07:00) Bangkok, Hanói, Yakarta
TZ_ID_73	(GMT+07:00) Krasnoyarsk
TZ_ID_74	(GMT+08:00) Pekín, Chongqing, Hong Kong, Urumchi
TZ_ID_75	(GMT+08:00) Irkutsk
TZ_ID_76	(GMT+08:00) Kuala Lumpur, Singapur
TZ_ID_77	(GMT+08:00) Perth
TZ_ID_78	(GMT+08:00) Taipéi
TZ_ID_79	(GMT+08:00) Ulán Bator
TZ_ID_80	(GMT+08:30) Pionyang
TZ_ID_81	(GMT+09:00) Osaka, Sapporo, Tokio
TZ_ID_82	(GMT+09:00) Seúl
TZ_ID_83	(GMT+09:00) Yakutsk
TZ_ID_84	(GMT+09:30) Adelaida
TZ_ID_85	(GMT+09:30) Darwin
TZ_ID_86	(GMT+10:00) Brisbane
TZ_ID_87	(GMT+10:00) Canberra, Melbourne, Sídney
TZ_ID_88	(GMT+10:00) Guam, Puerto Moresby
TZ_ID_89	(GMT+10:00) Hobart
TZ_ID_90	(GMT+10:00) Vladivostok
TZ_ID_91	(GMT+11:00) Magadán, Islas Salomón, Nueva caledonia
TZ_ID_92	(GMT+12:00) Auckland, Wellington
TZ_ID_93	(GMT+12:00) Fiyi
TZ_ID_94	(GMT+13:00) Nukualofa
TZ_ID_95	(GMT+14:00) Kiritimati
TZ_ID_96	(GMT+02:00) Atenas, Bucarest

Apéndice 2

Completar el archivo CSV de valor de pool

Tabla 13. Archivo de valor de pool

serviceTag (se completa automáticamente)	FQDD (se completa automáticamente)	poolAttributeName	poolAttributeValue
Etiqueta de servicio de los dispositivos desde los cuales se exportan los atributos específicos del sistema	Identifica el componente asociado al atributo específico del sistema	Identifica el atributo específico del sistema que se configurará	Establece el valor para el atributo específico del sistema especificado

Tabla 14. Ejemplos

serviceTag (se completa automáticamente)	FQDD (se completa automáticamente)	poolAttributeName	poolAttributeValue	Detalles sobre qué es el atributo y cómo completarlo
xxxxxxx	WINDOWS	HOSTNAME	WIN19SRVDTA	Qué: es el nombre de host que se configurará en el servidor implementado o provisionado.
xxxxxxx	WINDOWS	ServerMngNIC	<MAC Adresses>	Qué: es la dirección MAC del puerto de red que se puede comunicar con System Center y el dispositivo OMIMSSC. Cómo: vaya hasta el puerto específico para recuperar la dirección MAC desde iDRAC.
xxxxxxx	WINDOWS	LOGICALNETWORK	OSD MEDIANTE IP ESTÁTICA	Qué: es el perfil de red creado en SCVMM que conlleva el pool de direcciones IP estáticas, la subred y otros detalles de red que se aplicarán en MN Cómo: cree el perfil de red lógica en SCVMM y proporcione el nombre de la plantilla creada. Para obtener más información, consulte la sección Planificar la red Fabric de VMM en la documentación de Microsoft.
xxxxxxx	WINDOWS	IPSUBNET	100.100.28.0/22	Qué: es la máscara de subred para la entrada del pool de IP estática en el perfil de red lógica anterior.
xxxxxxx	WINDOWS	IPADDRESS	100.100.31.145	Qué: es la dirección IP estática que se aplicará en el nodo administrado implementado o provisionado.

Acceso a documentos desde el sitio de asistencia de Dell EMC

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

- Mediante los siguientes enlaces:
 - Para consultar documentos de Dell EMC Enterprise Systems Management, Dell EMC Remote Enterprise Systems Management y Dell EMC Virtualization Solutions, visite www.dell.com/esmanuals
 - Para consultar documentos de Dell EMC OpenManage, visite www.dell.com/openmanagemanuals
 - Para documentos de iDRAC, visite www.dell.com/idracmanuals
 - Para consultar documentos de Dell EMC OpenManage Connections Enterprise Systems Management, visite www.dell.com/OMConnectionsEnterpriseSystemsManagement
 - Para consultar documentos de Dell EMC Serviceability Tools, visite <https://www.dell.com/serviceabilitytools>
- En el sitio web de asistencia de Dell EMC:
 1. Vaya a <https://www.dell.com/support>.
 2. Haga clic en **Examinar todos los productos**.
 3. En la página **Todos los productos**, haga clic en **Software** y luego haga clic en el vínculo requerido de lo siguiente:
 - **Análisis**
 - **Administración de sistemas cliente**
 - **Aplicaciones empresariales**
 - **Administración de sistemas empresariales**
 - **Mainframe**
 - **Sistemas operativos**
 - **Soluciones para el sector público**
 - **Herramientas de servicio**
 - **Asistencia**
 - **Utilidades**
 - **Soluciones de virtualización**
 4. Para ver un documento, haga clic en el producto requerido y, luego, en la versión requerida.
- Mediante los motores de búsqueda:
 - Escriba el nombre y la versión del documento en el cuadro de búsqueda.