

Dell Lifecycle Controller Integration versión 1.3 para Microsoft System Center Virtual Machine Manager

Guía del usuario

1

Notas, precauciones y advertencias

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

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

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

Tabla de contenido

Capítulo 1: Acerca de Dell Lifecycle Controller Integration para Microsoft System Center Virtual Machine Manager.....	6
Novedades de esta versión.....	6
Funciones existentes.....	6
Capítulo 2: Instalación y configuración de complemento de la consola de DLCI.....	9
Instalación del complemento de la consola de DLCI.....	9
Extracción o reparación del complemento de la consola de DLCI.....	9
Importación del complemento de la consola de DLCI a VMM.....	10
Visualización del complemento de la consola de DLCI.....	10
Capítulo 3: Introducción.....	11
Iniciar sesión en el portal de administración de DLCI - SCVMM.....	11
Portal de administración de DLCI para SVMMe.....	11
Iniciar sesión en el complemento de consola de DLCI para SCVMM.....	12
Complemento de consola de DLCI para SCVMM.....	13
Capítulo 4: Flujos de trabajo.....	15
Acerca de las configuraciones doradas.....	15
Creación de configuraciones doradas.....	15
Creación, administración y eliminación de perfiles de credenciales.....	16
Creación, administración y eliminación de orígenes de actualización.....	16
Creación, administración y eliminación de grupos de actualización personalizados.....	16
Aplicación de actualizaciones en servidores.....	16
Creación, administración y eliminación de almacenes de protección.....	17
Exportación del perfil de servidor.....	17
Importación del perfil del servidor.....	17
Implementación de hipervisor.....	17
Eliminación de servidores.....	18
Configurar los componentes sustituidos.....	18
Recopilar y ver registros de LC.....	18
Capítulo 5: Configuración del entorno para la implementación de hipervisores.....	19
Capítulo 6: Detección de servidores.....	20
Requisitos del sistema para los sistemas administrados.....	21
Activación de CSIOR en Managed Systems.....	21
Descubrimiento de servidores mediante descubrimiento automático.....	21
Descubrimiento de servidores mediante descubrimiento manual.....	22
Eliminación de servidores de la consola de DLCI.....	22
Visualización de inventario del dispositivo.....	22
Sincronización con SCVMM.....	23
Sincronización del servidor con SCVMM.....	23
Resolución de errores de sincronización.....	23

Inicio de la consola de iDRAC.....	24
Capítulo 7: Licencia para el appliance.....	25
Capítulo 8: Administración del servidor.....	26
Integración con DRM.....	27
Filtros.....	27
Descripción general de origen de actualización.....	27
Configuración de FTP local.....	28
Configuración de HTTP local.....	28
Visualización del origen de actualizaciones.....	29
Creación de un origen de actualizaciones.....	29
Modificación del origen de actualizaciones.....	29
Eliminación de origen de actualizaciones.....	29
Grupos de actualización.....	30
Visualización grupos de actualización.....	31
Creación de grupos actualización personalizados.....	31
Modificación de grupos actualización personalizados.....	32
Eliminación de grupos actualización personalizados.....	32
Aplicación de actualizaciones en servidores.....	32
Sondeo y notificación.....	33
Configuración de notificaciones.....	33
Almacén de protección.....	34
Creación del almacén de protección.....	34
Modificación del almacén de protección.....	34
Eliminación del almacén de protección.....	34
Sustitución de piezas.....	34
Aplicar el firmware y los valores de configuración.....	35
Recopilación de registros del controlador Lifecycle.....	35
Recopilar registros de LC.....	35
Ver registros de LC.....	36
Exportación de inventario.....	36
Visualización y actualización de inventario de firmware.....	37
Exportación de perfiles de servidor.....	38
Creación de trabajos de exportación.....	38
Cancelación de trabajos de exportación de configuración de servidor.....	38
Importación del perfil del servidor.....	38
Importación del perfil del servidor.....	39
Administrar los trabajos.....	39
Cancelación de trabajos de actualización de firmware.....	39
Capítulo 9: Perfiles y plantillas.....	40
Acerca del perfil de credenciales.....	40
Creación de perfil de credenciales.....	41
Modificación de perfil de credenciales.....	41
Eliminación de un perfil de credenciales.....	41
Creación de perfil de hardware.....	41
Modificación de un perfil de configuración de hardware.....	42
Eliminación de perfil de hardware.....	42

Creación de perfil de hipervisor.....	43
Modificación de un perfil de hipervisor.....	43
Eliminación de perfil de hipervisor.....	43
Actualización de WinPE.....	43
Acerca de la implementación del hipervisor.....	44
Creación de plantilla de implementación.....	44
Modificación de una plantilla de implementación.....	45
Eliminación de una plantilla de implementación.....	45
Capítulo 10: Implementación de hipervisores.....	46
Capítulo 11: Visualización de información en el appliance.....	47
Centro de tareas y registros.....	47
Visualización de tareas administradas.....	48
Cancelar tareas programadas.....	48
Capítulo 12: Solución de problemas.....	49
El grupo de actualización de clúster vacío no se elimina durante el descubrimiento automático o la sincronización.....	49
Trabajos de descubrimiento no enviados.....	49
Creación de grupos de chasis VRTX duplicados.....	50
Exportación de perfil de configuración de otro servidor tras cambiar la dirección IP.....	50
Error al aplicar la configuración de RAID.....	50
Error de creación de origen de actualización.....	50
Error de actualización de firmware porque la de cola de trabajos está llena.....	50
Error al actualizar el firmware utilizando la fuente de actualización de DRM	51
Error de un trabajo programado en un grupo de actualización.....	51
Error de actualización del firmware en grupo actualización de clúster.....	51
Error al actualizar el firmware en 11.ª generación de servidores.....	51
Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema.....	52
Error al crear un repositorio durante una actualización del firmware.....	52
Error al eliminar un grupo de actualización personalizado.....	52
Error al exportar registros de LC en formato CSV.....	52
Error al ver los registros de LC	52
Error al exportar perfiles de servidores	52
Actualización del firmware en algunos componentes independientemente de la selección.....	53
Problema de instalación de IG mientras se ejecutan varias instancias del instalador en el mismo servidor	53
La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas.....	53
Error de implementación de hipervisores.....	53
Error de implementación del hipervisor debido a archivos de controlador retenidos en el recurso compartido de biblioteca.....	54
La información de inventario más reciente no aparece incluso después una actualización del firmware.....	54
Error 21119 de SCVMM VMM al agregar servidores Active Directory.....	54
La implementación del hipervisor falla en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory.....	55
Error de configuración de RAID para discos virtuales con RAID10.....	55
Error de configuración de RAID debido a la configuración de repuestos dinámicos en RAID de software S130....	55
Capítulo 13: Acceso a contenido de soporte desde el sitio de soporte de Dell EMC.....	56

Acerca de Dell Lifecycle Controller Integration para Microsoft System Center Virtual Machine Manager

Dell Lifecycle Controller Integration (DLCI) para Microsoft System Center Virtual Machine Manager (SCVMM) permite la configuración de hardware, brinda una solución para simplificar y mejorar el proceso de las actualizaciones de firmware y la implementación de hipervisores en los servidores Dell. Con este plug-in se utiliza la función de implementación remota de Integrated Dell Remote Access Controller (iDRAC) con Lifecycle Controller (LC), lo que proporciona una experiencia de usuario sin problemas. Puede aprovechar las adiciones de valor de Dell a través de consolas de Microsoft System Center para administrar los entornos virtualizados.

Para obtener información acerca de Microsoft System Center Virtual Machine Manager, consulte la documentación de Microsoft.

Temas:

- [Novedades de esta versión](#)
- [Funciones existentes](#)

Novedades de esta versión

Las funciones de esta versión son las siguientes:

- Exportar inventario en formato CSV: después de comparar los inventarios de los servidores la fuente de la actualización, puede exportar el informe de comparación al archivo CSV.
- Reemplazo de piezas: restauración de la versión del firmware, o configuración, o bien ambas en el nuevo componente del servidor.
- Recopilar y Ver mensajes de registros de LC: exportación, visualización, descarga en formato CSV, y búsqueda en los mensajes de registros de LC mensajes.
- Tareas y registros de actividades: mejora de la presentación de los trabajos y los registros de actividades para mejorar la experiencia de usuario.
- Implementación de Windows Server 2016: compatibilidad con la implementación de Windows Server 2016.
- Paquetes de actualización de Dell de 64 bits (DUP): compatibilidad para actualizar la versión de firmware utilizando DUP de 64 bits.
- Compatibilidad con System Center 2016 Virtual Machine Manager (SC2016 VMM): puede instalar DLCI para SCVMM en SC2016 VMM.

Funciones existentes

Con DLCI para SCVMM, puede continuar haciendo lo siguiente:

- Orígenes de actualización: cree un repositorio utilizando DRM, o mediante la conexión a un sitio FTP.
 - Integración con DRM: exporte la información del inventario del sistema de DLCI para SCVMM a DRM y utilice DRM para preparar un repositorio.
 - FTP: conéctese con el sitio FTP de Dell (local o en línea) y obtenga los catálogos en línea de Dell más recientes.
 - HTTP: compatibilidad con el tipo Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto, HTTP) de fuente de actualización.
- Probar conexión: validación de la ubicación de origen de actualización y las credenciales antes de crear la fuente de actualización.
- Grupos de actualización: agrupación de los servidores para crear, administrar y realizar las actualizaciones de firmware en grupos de actualización personalizados.
- Sondeo y notificaciones: configure notificaciones para recibir alertas cuando haya disponibles nuevos catálogos en el origen de actualización.
- Almacenes de protección: ubicación para guardar perfiles de configuración del sistema.

- Exportar perfiles de servidores, incluidas las imágenes de firmware en componentes como, por ejemplo, el Sistema básico de entrada/salida (BIOS), la matriz redundante de discos independientes (RAID), la Network Interface Controller (controladora de interfaces de red, NIC), la Integrated Dell Remote Access Controller (iDRAC), LC, etc., a una ubicación interna o externa.
- Importar perfiles de servidor: conservar o excluir la configuración de RAID actual para el mismo servidor o los mismos grupos de servidores cuando el perfil de servidor existente está dañado.
- Filtros: se utilizan para mostrar información basada en los criterios seleccionados en el **Maintenance Center (Centro de mantenimiento)**.
- Permitir degradación: si se habilita, le permite degradar la versión de firmware a una versión anterior.
- Cluster-Aware Updating (CAU, actualización compatible en clústeres): automatiza el proceso de actualización de software mediante el uso de las funciones de Microsoft en grupos de actualización de clúster manteniendo la disponibilidad del servidor.
- Integración con Dell Repository Manager (DRM): el suministro de la información del inventario de servidor de los servidores existentes del servidor a DRM.
- Detectar automáticamente servidores Dell sin asignar: conecte los servidores Dell entregados de fábrica a la red, enciéndalos e introduzca los detalles del servidor de aprovisionamiento del servidor DLCI para que detecte automáticamente los servidores.

Los servidores descubiertos por el servidor se conocen como servidores sin asignar y están disponibles para la implementación de hipervisores.

- Descubrir manualmente servidores Dell sin asignar: descubra los servidores PowerEdge de 11.^ª, 12.^ª y 13.^ª generación e impleméntelos en un entorno virtual.
- Ver el inventario de servidores descubiertos: se proporcionan detalles clave de inventario acerca los servidores Dell.
- Comprobar el cumplimiento del servidor: para usar las funciones disponibles en el dispositivo, los servidores Dell deben tener las versiones del firmware necesarias de iDRAC, LC y el sistema básico de entrada/salida (BIOS). Para obtener información sobre los números de versión, consulte *Notas de la versión DLCI para SCVMM*.
- Preparar una configuración del servidor ideal, también conocida como configuración dorada: replique esta configuración en los servidores implementados en el entorno virtual. También puede:
 - Editar y modificar la configuración de oro para el orden de inicio y el BIOS.
 - Personalizar la estrategia de repuestos dinámicos dedicados (DHS) para RAID.
- Crear y mantener perfiles y plantillas.
- Personalizar el entorno de preinstalación de Microsoft Windows (WinPE): prepare imágenes WinPE personalizadas con los controladores más recientes de Dell OpenManage Deployment Toolkit (DTK).
- Usar la función de inyección de controladores de LC para los servidores entregados de fábrica más recientes que se envían con los paquetes de controladores más recientes.

Implementar hipervisores con o sin la inyección de controladores de LC: desde el servidor, implemente hipervisor en función de la configuración dorada.

- Iniciar la consola de iDRAC desde la consola de DLCI para ver información de inventario y solucionar problemas.
- Licenciamiento simplificado: ya no requiere Dell Connections License Manager (DCLM) para administrar sus licencias. Puede obtener más información sobre el licenciamiento en el portal de administración **Centro de licencias**.
- Tipos de perfil de credenciales nuevos:
 - Perfil de credenciales del dispositivo: se utiliza para iniciar sesión en el iDRAC o en Chassis Management Controller (CMC).
 - Perfil de credenciales de Windows: utilícelo para acceder a los recursos compartidos de Windows.
 - Perfil de credenciales de FTP: utilícelo para acceder al sitio FTP.
 - Credenciales del servidor proxy: utilícelas para proporcionar las credenciales de proxy.
- Detección: detecte servidores con los detalles de clúster si el host forma parte de un clúster, y detalles de chasis si se trata de un servidor modular.
- Sincronizar con SCVMM: sincronización de todos los sistemas host de Dell que se enumeran en el entorno de SCVMM con DLCI para SCVMM, donde los hosts son hosts Hyper-V administrados por SCVMM.
 - Resolver errores de sincronización: vuelva a sincronizar los servidores host que no se sincronizaron durante un intento anterior.
- Administración del servidor: administre servidores Dell en entornos SCVMM y manténgalos actualizados según las recomendaciones de Dell en función del firmware más reciente y otras actualizaciones. La administración de servidores desde la 11.^ª a la 13.^ª generación de servidores Dell PowerEdge está soportada.
 - Las funciones clave de la administración de servidores son las siguientes:
 - Visualización del informe de comparación: vea los informes de comparación con importancia desde una fuente de actualización y, a continuación, cree una versión base. La importancia se refiere a la relevancia de la actualización.
 - Actualizar y exportar el inventario del firmware: actualice el inventario del firmware y exporte sus detalles en formato xml.
 - Aplicación de actualizaciones: aplique las actualizaciones de firmware o programe las actualizaciones.

- Aplicar actualizaciones específicas: aplique solo las actualizaciones de componentes específicos o aplique la actualización más reciente disponible en el sitio FTP de Dell.
- Aplicación de las actualizaciones antes de la implementación del sistema operativo: antes de implementar un sistema operativo, aplique las actualizaciones de firmware mediante un origen de actualización adecuado.
- Actualizar de forma remota servidores (de uno a uno o de uno a muchos) para las versiones de firmware más recientes de lo siguiente:
 - BIOS
 - NIC o LAN en placa base (LOM)
 - Unidades de suministro de energía (PSU) de servidores PowerEdge de 12.ª generación en adelante
 - Controladora RAID PowerEdge (PERC) o SCSI de conexión en serie (SAS)
 - Plano posterior
 - IDRAC (modulares y monolíticos) con LC

 **NOTA:** Los componentes disponibles se enumeran en los servidores Dell.

Instalación y configuración de complemento de la consola de DLCI

La instalación y configuración del complemento de la consola de DLCI para SCVMM incluye lo siguiente:

- Revise y complete los requisitos del sistema y, a continuación, instale el **Complemento de la consola de DLCI para SCVMM**. Para obtener más información, consulte [Instalación del complemento de la consola de DLCI](#).
- Importe la consola de DLCI a la consola de VMM: Para obtener más información, consulte [Importación de la consola de DLCI a la consola de VMM](#).
- Ver la consola de DLCI en la consola de VMM. Para obtener más información, consulte [Visualización de la consola de DLCI](#).

Temas:

- [Instalación del complemento de la consola de DLCI](#)
- [Extracción o reparación del complemento de la consola de DLCI](#)
- [Importación del complemento de la consola de DLCI a VMM](#)
- [Visualización del complemento de la consola de DLCI](#)

Instalación del complemento de la consola de DLCI

Antes de comenzar a trabajar con el dispositivo, instale la consola de DLCI en el sistema en donde está instalada la consola de SCVMM. Una vez que instale la consola de DLCI, puede importar la consola de DLCI a la consola de SCVMM.

Requisitos previos: que esté instalada la consola de SC2012 VMM R2, SC2012 VMM SP1 o SC2016 VMM.

Si va a instalar la consola de DLCI por primera vez desde **Setup and Configuration (Instalación y configuración)**, comience en el paso 3; de lo contrario, comience en el paso 1.

Para instalar la consola de DLCI, realice los pasos siguientes:

1. En **Portal de administración de DLCI - SCVMM**, haga clic en **Descargas**.
2. En **Instalador de complemento de consola de DLCI para SCVMM**, haga clic en **Descargar instalador** y guarde el archivo en una ubicación.
3. Ejecute el archivo del instalador.
4. En la página de bienvenida del **Complemento de consola de DLCI para SCVMM**, haga clic en **Siguiente**.
5. En la pantalla **Contrato de licencia**, seleccione **Acepto los términos del contrato de licencia** y, a continuación, haga clic en **Siguiente**.
6. En la ventana **Carpeta de destino**, hay una carpeta de instalación seleccionada de manera predeterminada. Para cambiar la ubicación, haga clic en **Cambiar**, complete los cambios y, a continuación, haga clic en **Siguiente**.
7. En la página **Preparado para instalar el programa**, haga clic en **Instalar**.
8. En la página **Asistente InstallShield completado**, haga clic en **Terminar**.

Extracción o reparación del complemento de la consola de DLCI

Para extraer o reparar el complemento de la consola de DLCI, realice los pasos siguientes:

1. Ejecute el instalador del **complemento de consola de DLCI para SCVMM**.
2. En **Mantenimiento de programas**, seleccione **Quitar** o **Reparar** y, a continuación, haga clic en **Siguiente**.
3. En **Listo para reparar o quitar el programa**, haga clic en **Instalar**.
4. Cuando finalice la tarea de extracción o reparación, haga clic en **Terminar**.

Importación del complemento de la consola de DLCI a VMM

Para trabajar con el servidor de DLCI, importe la consola de DLCI a la consola de VMM.


Requisitos previos: para que la conexión con el servidor de DLCI funcione, en el explorador de web, borre la configuración de proxy; no obstante, si los valores de proxy del explorador de web están configurados, incluya el nombre de dominio completo (FQDN) del servidor en la lista de excepciones de proxy.

Para importar la consola de DLCI a la consola de VMM:

1. En SCVMM, haga clic en **Configuración**.
2. En la cinta **Inicio**, haga clic en **Importar complemento de consola**.
3. Haga clic en **Asistente para importar el complemento de consola** > **Seleccionar un complemento para importar**, examine para seleccionar el complemento de consola de DLCI para SCVMM (**DLCI_VMM_Console_Addin.zip**) y, a continuación, haga clic en **Siguiente**.
4. En **Confirmar la configuración**, confirme que los ajustes sean los necesarios y, a continuación, haga clic en **Terminar**. La consola de DLCI se importa a la consola de VMM y está disponible en **VMs and Services (Máquinas virtuales y servicios)** > **All Hosts (Todos los hosts)**.

Visualización del complemento de la consola de DLCI

Para ver el complemento de consola de DLCI en SCVMM:

1. En la consola de SCVMM, seleccione **Fabric** y, a continuación, seleccione **Todos los grupos de hosts**.
 **NOTA:** Para iniciar la consola de DLCI, puede seleccionar cualquier grupo de hosts al que tenga acceso.
2. En la cinta **Inicio**, seleccione **Consola de DLCI**.

Introducción

Los sistemas de administración son los sistemas donde está instalado DLCI para SCVMM, también conocido como el dispositivo y sus componentes. A continuación, se presentan los componentes del dispositivo:

- Puerta de enlace de Dell Lifecycle Controller Integration (DLCI) para Microsoft System Center Virtual Machine Manager (SCVMM), también conocido como puerta de enlace de integración de DLCI para SCVMM.
- El complemento de consola de Dell Lifecycle Controller Integration (DLCI) para Microsoft System Center Virtual Machine Manager (SCVMM), también se conoce como complemento de consola de DLCI para SCVMM.

Temas:

- [Iniciar sesión en el portal de administración de DLCI - SCVMM](#)
- [Portal de administración de DLCI para SVMMeI](#)
- [Iniciar sesión en el complemento de consola de DLCI para SCVMM](#)
- [Complemento de consola de DLCI para SCVMM](#)

Iniciar sesión en el portal de administración de DLCI - SCVMM

Para iniciar sesión en el portal de administración de DLCI - SCVMM, realice los pasos siguientes:

1. Desde el dispositivo, observe el URL del portal de administración de DLCI - SCVMM.
2. En un navegador web, acceda a la siguiente URL: `https://<IP Address> o <FQDN>`.
Por ejemplo: `192.168.20.30 o DLCIforSCVMM.myorgdomain.com`.
3. Inicie sesión en el portal de administración de DLCI - SCVMM con las credenciales de usuario proporcionadas al configurar el dispositivo.

Portal de administración de DLCI para SVMMeI

La interfaz de usuario del portal de administración de DLCI - SCVMM contiene las siguientes opciones:

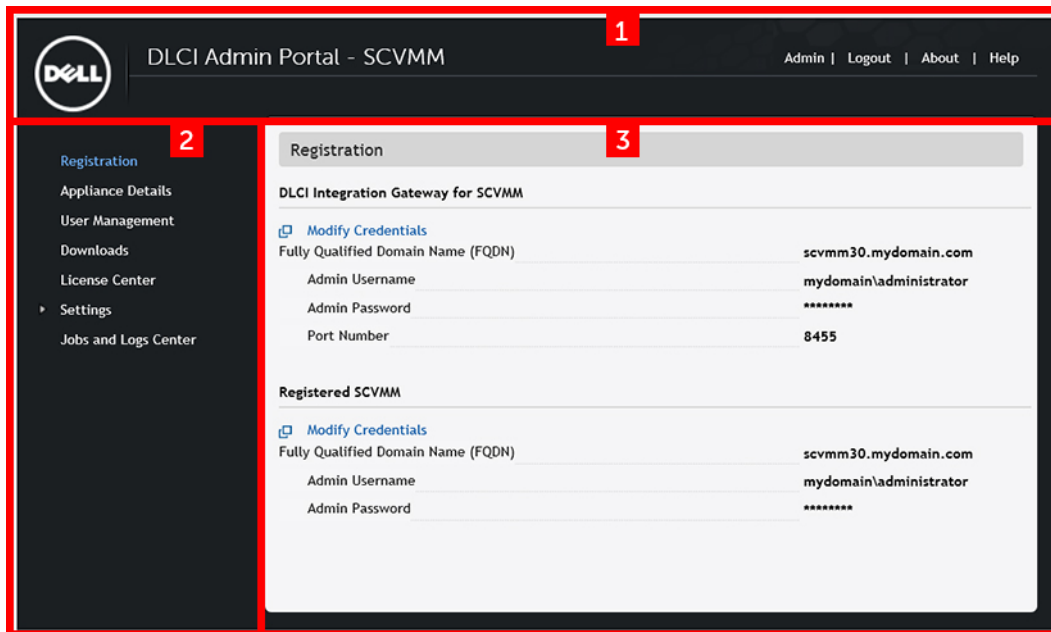


Ilustración 1. Portal de administración de DLCI - SCVMM

- El banner de encabezado incluye el nombre del producto y las siguientes opciones:
 - **Administrador**: muestra información sobre el usuario que ha iniciado sesión en el portal de administración de DLCI para SCVMM.
 - **Logout (Cerrar sesión)**: le permite cerrar sesión en el portal de administración de DLCI para SCVMM.
 - **About (Acerca de)**: proporciona información sobre la versión de DLCI para SCVMM.
 - **Help (Ayuda)**: inicia la ayuda contextual en línea.
- El panel de navegación contiene las siguientes opciones. Para obtener más información sobre estas opciones, consulte la Ayuda en línea.
 - **Registro**
 - **Detalles del dispositivo**
 - **Administración de usuarios**
 - **Descargas**
 - **Centro de licencias**
 - **Configuración**
 - **Actualizaciones de Service Pack**
 - **Registros**
 - **Centro de tareas y registros**
- El área de consola muestra información acerca de la opción seleccionada en el panel de navegación.

Iniciar sesión en el complemento de consola de DLCI para SCVMM

Para iniciar sesión en el complemento de consola de DLCI para SCVMM:

- En SCVMM, seleccione **Fabric** y, a continuación, seleccione **Todos los hosts**.
- En la cinta **Inicio**, seleccione **Consola de DLCI**.

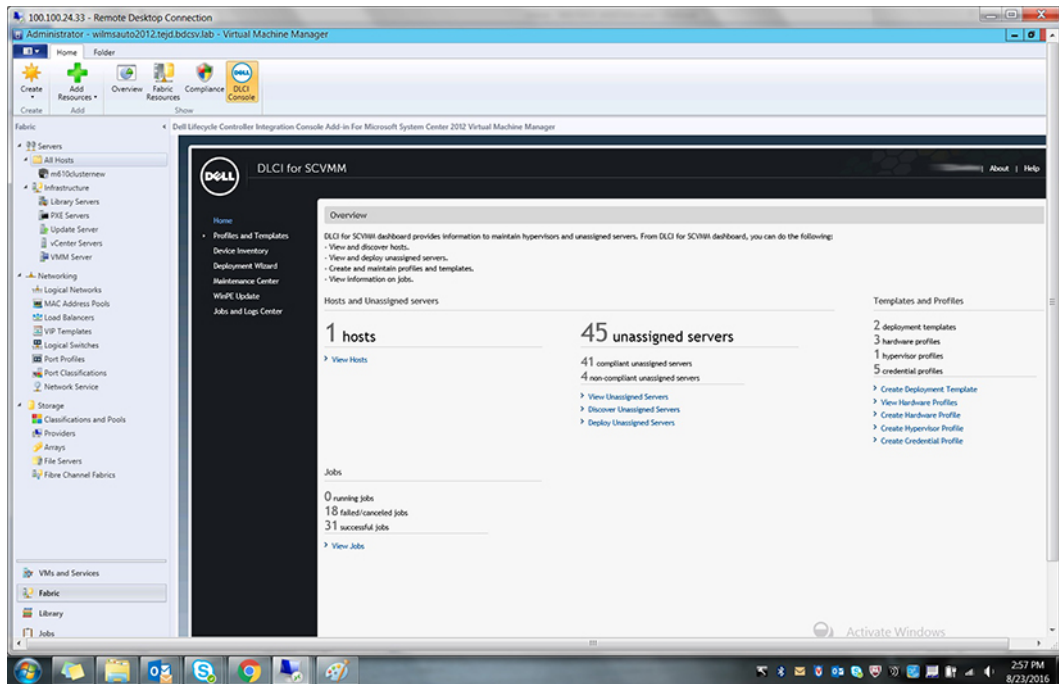


Ilustración 2. –Complemento de consola de DLCI para SCVMM

Complemento de consola de DLCI para SCVMM

La interfaz de usuario del complemento de consola de DLCI contiene las siguientes opciones:

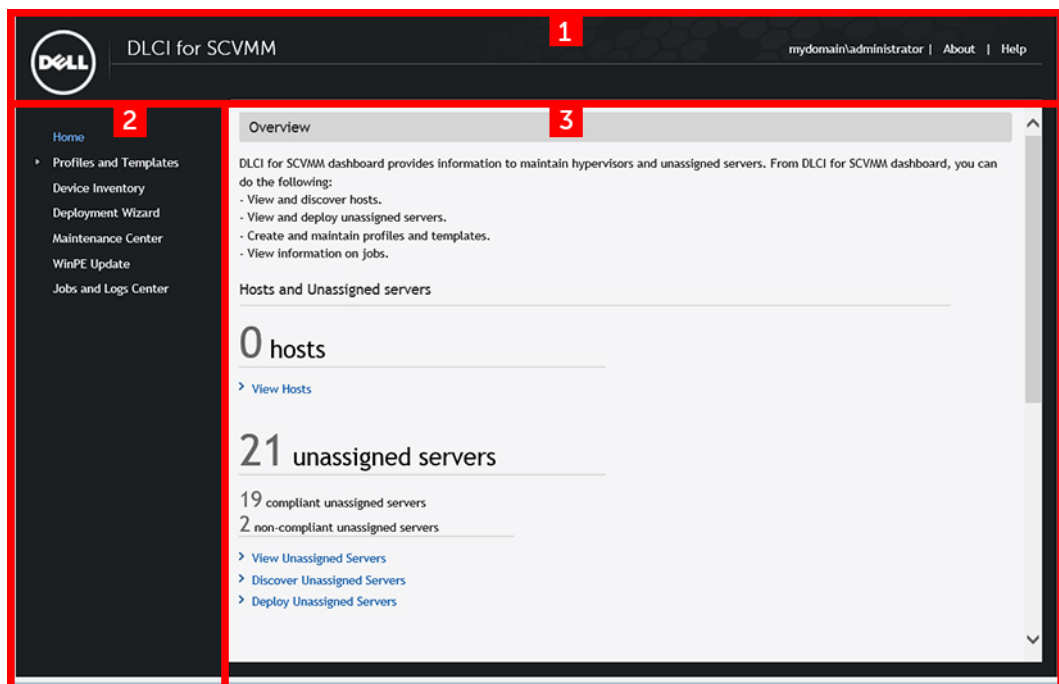


Ilustración 3. Complemento de consola de DLCI para SCVMM

1. El banner de encabezado contiene el nombre del producto y las siguientes opciones:
 - **<Domain>\administrator (<Dominio>\administrador)**: muestra información sobre el usuario que ha iniciado sesión en DLCI para SCVMM.
 - **About (Acerca de)**: proporciona información sobre la versión de DLCI para SCVMM.
 - **Help (Ayuda)**: inicia la ayuda contextual en línea.

2. El panel de navegación contiene las siguientes opciones:

- **Home (Inicio):** muestra el panel de DLCI para SCVMM.
- **Perfiles y plantillas**
 - **Plantilla de implementación**
 - **Perfil de hardware**
 - **Perfil de hipervisor**
 - **Perfil de credenciales**
- **Inventario de dispositivos**
- **Asistente de implementación**
- **Centro de mantenimiento**
- **Actualización de WinPE**
- **Centro de tareas y registros**

3. El área de consola muestra información acerca de la opción seleccionada en el panel de navegación.

i **NOTA:** En la consola de DLCI para SCVMM, si está trabajando en un asistente, por ejemplo el asistente de perfil de hardware, y navega hacia otra ficha u otro vínculo en la consola de DLCI SCVMM y visualiza el complemento de la consola de DLCI para SCVMM nuevamente, la información proporcionada no se guarda y la consola de DLCI muestra la **página de inicio**.

Flujos de trabajo

Esta sección contiene los siguientes flujos de trabajo:

- Creación de configuraciones doradas
- Creación y administración de perfiles de credenciales
- Creación y administración de orígenes de actualizaciones
- Creación y administración de grupos de actualización personalizados
- Aplicación de actualizaciones en servidores
- Implementación de hipervisores
- Creación, administración y eliminación de almacenes de protección
- Exportación de perfiles de servidor
- Importación de perfiles de servidores
- Eliminación de servidores
- Configurar los componentes sustituidos
- Recopilar y ver registros de LC

Temas:

- Acerca de las configuraciones doradas
- Creación de configuraciones doradas
- Creación, administración y eliminación de perfiles de credenciales
- Creación, administración y eliminación de orígenes de actualización
- Creación, administración y eliminación de grupos de actualización personalizados
- Aplicación de actualizaciones en servidores
- Creación, administración y eliminación de almacenes de protección
- Exportación del perfil de servidor
- Importación del perfil del servidor
- Implementación de hipervisor
- Eliminación de servidores
- Configurar los componentes sustituidos
- Recopilar y ver registros de LC

Acerca de las configuraciones doradas

Una configuración del servidor con la secuencia de arranque preferido y con los ajustes de BIOS y RAID ideales para la organización se denomina configuración dorada. Estos ajustes se recopilan en un perfil de hardware y se implementan en servidores idénticos durante las implementaciones del hipervisor.

Creación de configuraciones doradas

Para preparar y utilizar una configuración dorada:

1. Asegúrese de que se haya descubierto y esté disponible el servidor con la configuración ideal. Para obtener más información sobre el descubrimiento de servidores, según el requisito, consulte [Descubrimiento de servidores mediante el descubrimiento automático](#) o [Descubrimiento de servidores mediante el descubrimiento manual](#).

2. Asegúrese de que el inventario del servidor esté actualizado. Para obtener más información, consulte [Visualización y actualización del inventario del firmware](#).
3. Para registrar la configuración ideal, cree un perfil de hardware. Para crear un perfil de hardware, consulte [Creación de un perfil de hardware](#).
4. Si desea modificar las configuraciones, consulte [Modificación de un perfil de configuración de hardware](#).

Creación, administración y eliminación de perfiles de credenciales

Para crear un perfil de credenciales, consulte [Creación de un perfil de credenciales](#).

Para administrar un perfil de credenciales, consulte [Modificación de un perfil de credenciales](#).

Para eliminar un perfil de credenciales, consulte [Eliminación de un perfil de credenciales](#).

Creación, administración y eliminación de orígenes de actualización

Para crear un origen de actualización, consulte [Creación de un origen de actualización](#).

Para administrar un origen de actualización, consulte [Modificación de un origen de actualización](#).

Para eliminar un origen de actualización, consulte [Eliminación de un origen de actualización](#).

Creación, administración y eliminación de grupos de actualización personalizados

Para crear un grupo de actualización personalizado, consulte [Creación de un grupo de actualización personalizado](#).

Para administrar un grupo de actualización personalizado, consulte [Modificación de un grupo de actualización personalizado](#).

Para eliminar un grupo de actualización personalizado, consulte [Eliminación de un grupo de actualización personalizado](#).

Aplicación de actualizaciones en servidores

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

- FTP en línea y origen de FTP local.
- HTTP en línea y HTTP local
- Repositorio DRM local

Para aplicar actualizaciones en servidores o grupos de servidores seleccionados:

1. Antes de comenzar las actualizaciones, vea la información sobre las fuentes y los grupos de actualización. Para obtener más información, consulte [Administración del servidor](#).
2. Descubrir servidores Para obtener más información, consulte [Descubrimiento de servidores mediante el descubrimiento automático o Descubrimiento de servidores mediante el descubrimiento manual](#).
3. Sincronizar los servidores presentes en el entorno SCVMM con DLCI para SCVMM. Para obtener más información sobre la sincronización, consulte [Sincronización con SCVMM](#).
4. Asegúrese de que el inventario de los servidores esté actualizado. Para obtener más información, consulte [Visualización del inventario del dispositivo](#).
5. Asegúrese de que se haya creado una fuente de actualización. Para obtener más información, consulte [Creación de una fuente de actualización](#).
6. Asegúrese de que la fuente de actualización se actualiza periódicamente con el catálogo más reciente mediante sondeo y notificaciones. Para obtener más información, consulte [Sondeo y notificación](#).

7. Asegúrese de que los grupos de servidores necesarios estén seleccionados para aplicar las actualizaciones. Para obtener más información, consulte [Aplicación de actualizaciones en servidores](#).

NOTA: Seleccione **Permitir degradación** para degradar la versión de firmware de los componentes.

Creación, administración y eliminación de almacenes de protección

1. Para crear un almacén de protección, consulte [Creación de almacén de protección](#).
2. Para administrar un almacén de protección, consulte [Modificación de almacén de protección](#).
3. Para eliminar un almacén de protección, consulte [Eliminación de almacén de protección](#).

Exportación del perfil de servidor

Para exportar la configuración del servidor:

1. Cree un almacén de protección. Para obtener más información, consulte [Creación de un vault de protección](#).
2. Exportar el perfil de servidor inmediatamente o programarlo para una fecha posterior. Para obtener más información, consulte [Creación de trabajos de exportación](#).

Importación del perfil del servidor

Para importar un perfil de servidor:

1. Cree un almacén de protección. Para obtener más información, consulte [Creación de un vault de protección](#).
2. Exporte un perfil de servidor. Para obtener más información, consulte [Creación de trabajos de exportación](#).
3. Importe un perfil de servidor exportado que incluya o excluya la configuración de RAID. Para obtener más información, consulte [Importación de un perfil de servidor](#).

Implementación de hipervisor

Mediante el dispositivo, puede realizar la actualización del firmware y la implementación del hipervisor según la configuración dorada. Puede usar la función de inyección de controladores de LC para los servidores entregados de fábrica que se envían con los paquetes de controladores más recientes. Además, puede actualizar los paquetes de controladores y obtener los mismos beneficios que instalar los controladores más recientes durante las implementaciones del hipervisor y las actualizaciones del firmware.

Tabla 1. Diferentes escenarios para la implementación de hipervisores

Si necesita los controladores de fábrica más reciente y los controladores fuera de banda	Al crear un perfil del hipervisor, active LC Driver Injection.
Si desea conservar la configuración de hardware existente	Al crear una plantilla de implementación, seleccione solo el perfil de hipervisor.

Para trabajar con la implementación de hipervisor, consulte lo siguiente:

1. [Acerca de la implementación](#)
2. [Creación de perfiles de credenciales](#)
3. [Creación de orígenes de actualización](#)
4. [Creación de perfiles de hardware](#)
5. [Creación de perfiles de hipervisor](#)
6. [Creación de plantillas de implementación](#)
7. (Opcional) [Creación de grupos actualización personalizados](#)
8. (Opcional) [Aplicación de actualizaciones en servidores](#)
9. [Implementación de hipervisores](#)

Eliminación de servidores

Para obtener información sobre la eliminación de servidores en el servidor, consulte [Eliminación de servidores de la consola de DLCI](#).

Configurar los componentes sustituidos

Para actualizar los componentes de servidor sustituidos a la versión de firmware requerida o la configuración de un componente antiguo, o ambos, consulte [Sustitución de piezas](#).

Recopilar y ver registros de LC

Para exportar y ver los archivos, consulte [Recopilar registros de LC](#).

Configuración del entorno para la implementación de hipervisores

Para configurar un entorno para la implementación de hipervisores:

1. Prepare [Configuraciones doradas](#).
2. Cree un perfil de computadora física en SCVMM. Para obtener más información, consulte la documentación de SCVMM.
3. Cree un grupo host objetivo en SCVMM. Para obtener más información, consulte la documentación de SCVMM.
4. Descargue la versión más reciente de Dell Deployment ToolKit (DTK) y cree una imagen ISO de arranque del entorno de preinstalación de Windows (WinPE). Para obtener más información, consulte [Actualización de WinPE](#).
5. Configure los sistemas para el descubrimiento automático. Para obtener más información, consulte [Descubrir servidores mediante el descubrimiento automático](#).
6. (Opcional) Cree una fuente de actualización. Para obtener más información, consulte [Creación de una fuente de actualización](#).
7. (Opcional) Cree grupos de actualización personalizados. Para obtener más información, consulte [Creación de un grupo de actualización personalizado](#).
8. (Opcional) Cree un perfil de hardware. Para obtener más información, consulte [Creación de un perfil de hardware](#).
9. Cree un perfil de hipervisor. Para obtener más información, consulte [Crear un perfil de hipervisor](#).
10. Cree una plantilla de implementación. Para obtener más información, consulte [Creación de una plantilla de implementación](#).
11. Una vez que los sistemas se descubren y están disponibles en el dispositivo, realice la actualización del firmware (opcional) y, a continuación, realice la implementación del hipervisor. Para obtener más información sobre la aplicación de actualizaciones, consulte [Aplicación de actualizaciones en servidores](#). Para obtener más información sobre la implementación del hipervisor, consulte [Implementación de hipervisores](#).
12. Vea el estado del trabajo de la actualización y la implementación del firmware. Para obtener más información, consulte [Centro de trabajos y registros](#).

Detección de servidores

Puede detectar servidores Dell sin asignar fuera de banda e importar información sobre los servidores Dell al dispositivo.

Puede descubrir hosts Hyper-V y hosts Hyper-V modulares junto con servidores sin asignar. Después del descubrimiento, los servidores se agregan a los respectivos grupos de actualización predefinidos. Para obtener más información sobre la clasificación de grupos de servidores, consulte [Administración de servidores](#).

Notas sobre la detección de servidores:

- Si se detecta un servidor Dell PowerEdge con un sistema operativo ya presente en SCCM o SCVMM, el servidor aparece como un servidor host y está marcado como compatible o no compatible.
 - Un servidor host es compatible cuando tiene las versiones mínimas de firmware de LC, iDRAC y BIOS necesarias para trabajar con el servidor.
 - Si el host es un servidor modular, la etiqueta de servicio del chasis que contiene el servidor también se muestra.
 - Si el host forma parte de un clúster, se muestra el nombre de dominio completo (FQDN) del clúster.
- Si se detecta un servidor Dell PowerEdge que no aparece en la lista de SCCM o SCVMM, el servidor aparece como un servidor sin asignar marcado como compatible o incompatible según sus versiones de firmware de LC, iDRAC, y el BIOS.
- Si proporciona detalles de credenciales incorrectos, en función de la versión de iDRAC, están disponibles las resoluciones siguientes:
 - Al detectar un servidor Dell PowerEdge de 12.ª generación con la versión de iDRAC 2.10.10.10 o posterior, si se proporcionan detalles incorrectos del perfil de credenciales, fallará la detección del servidor con el siguiente comportamiento:
 - Para el primer intento, no se bloquea la dirección IP del servidor.
 - Para el segundo intento, se bloquea la dirección IP del servidor durante 30 segundos.
 - Para el tercer intento y para intentos posteriores, se bloquea la dirección IP del servidor durante 60 segundos.
 Puede intentar descubrir el servidor con detalles correctos del perfil de credenciales cuando se desbloquea la dirección IP.
 - Al detectar de un servidor PowerEdge de 11.ª o 12.ª generación con versiones de iDRAC anteriores a la 2.10.10.10, si los intentos de detección del servidor fallan por haber introducido detalles incorrectos del perfil de credenciales, vuelva a detectar el servidor con los detalles correctos del perfil de credenciales.
 - En el caso de las versiones de iDRAC anteriores a 2.10.10.10, se puede configurar el bloqueo de las direcciones IP. Para obtener más información, consulte la documentación de iDRAC en Dell.com/idracmanuals. Según sus requisitos, también puede deshabilitar el bloqueo de las direcciones IP. Además, puede verificar si la función `iDRAC.IPBlocking.BlockEnable` está activada en iDRAC.
 - 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.

También puede detectar servidores Dell sin asignar mediante las siguientes opciones:

- [Detección automática](#) de servidores sin asignar.
- [Detección manual](#) basada en direcciones IP.

Temas:

- [Requisitos del sistema para los sistemas administrados](#)
- [Activación de CSIOR en Managed Systems](#)
- [Descubrimiento de servidores mediante descubrimiento automático](#)
- [Descubrimiento de servidores mediante descubrimiento manual](#)
- [Eliminación de servidores de la consola de DLCI](#)
- [Visualización de inventario del dispositivo](#)
- [Sincronización con SCVMM](#)
- [Sincronización del servidor con SCVMM](#)
- [Resolución de errores de sincronización](#)
- [Inicio de la consola de iDRAC](#)

Requisitos del sistema para los sistemas administrados

Los sistemas administrados son sistemas que se administran mediante el dispositivo. Para que el dispositivo descubra los sistemas administrados, se necesitan los requisitos del sistema que se indican a continuación:

- Para los servidores Dell PowerEdge de 11.ª, 12.ª y 13.ª generación, el servidor admite solo modelos de servidores modulares y monolíticos.
- Para la configuración de origen y de destino, utilice el mismo tipo de discos (solo Unidad de estado sólido (SSD), SAS o solo las unidades de serie 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 el modo de inicio de la Interfaz de firmware extensible unificada (UEFI).
- 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 [Activación de CSIOR en sistemas administrados](#).

Activación de CSIOR en Managed Systems

Para activar CSIOR en los servidores Dell PowerEdge de 12.ª y 13.ª generación:

1. Presione **F2** durante la POST para entrar a **Configuración del sistema**.
2. Seleccione **iDRAC Settings Configuración de iDRAC** y haga clic en **Lifecycle Controller**.
3. Para **Recopilar inventario del sistema al reiniciar (CISOR)**, establezca el valor en **Habilitado**.

Para activar CSIOR en los servidores PowerEdge de 11.ª generación:

1. Reinicie el sistema.
2. Durante la autoprueba de encendido (POST), cuando el sistema le indique que especifique la utilidad iDRAC, pulse **CTRL + E**.
3. De las opciones disponibles, seleccione **Servicios del sistema** y pulse **Intro**.
4. Seleccione **Recopilar inventario del sistema al reiniciar** y presione las teclas de dirección derecha o abajo y establézcalo como **Habilitado**.

Descubrimiento de servidores mediante descubrimiento automático

Conecte los servidores Dell a la red y encienda los servidores para que el servidor de DLCI descubra automáticamente los servidores. El servidor descubre automáticamente servidores Dell sin asignar mediante la función de activación remota del iDRAC. El appliance funciona como el servidor de aprovisionamiento y utiliza la referencia del iDRAC para descubrir servidores Dell automáticamente.

Para realizar el descubrimiento automático en los servidores Dell:

1. En el dispositivo, cree un perfil de credenciales del tipo de dispositivo (especificando las credenciales de iDRAC y marcándolas como valor predeterminado) para los servidores Dell. Para obtener más información, consulte [Creación de un perfil de credenciales](#).
2. En los servidores Dell que desea descubrir automáticamente, realice lo siguiente:
 - a. Desactive las cuentas de administrador existentes en iDRAC.
 - b. En la configuración del iDRAC, en activación remota, habilite Auto-Discovery (Detección automática).
 - c. Después de activar el descubrimiento automático, proporcione la dirección IP del servidor de aprovisionamiento (que es el appliance de DLCI) y reinicie el servidor.

Descubrimiento de servidores mediante descubrimiento manual

Puede descubrir manualmente los servidores mediante una dirección IP o un rango IP. Para descubrir servidores, proporcione la dirección IP de iDRAC y las credenciales del tipo de dispositivo de los servidores. Cuando se descubren servidores mediante un rango IP, especifique un rango IP (IPv4) (dentro de una subred).

Para descubrir servidores Dell manualmente:

1. En Complemento de consola de DLCI para SCVMM, realice alguna de las acciones siguientes:
 - En el escritorio, haga clic en **Descubrir servidores sin asignar**.
 - En el panel de navegación, haga clic en **Inventario de dispositivos** y en **Inventario**, haga clic en **Descubrir**.
2. En **Descubrir**, seleccione la opción necesaria:
 - **Descubrir mediante una dirección IP**
 - **Descubrir mediante un rango IP**
3. Seleccione el perfil de credenciales de tipo de dispositivo necesario, o haga clic en **Crear nuevo** para crear un perfil de credenciales.
4. En **Detectar mediante una dirección IP o un rango de direcciones IP**, realice alguna de las acciones siguientes:
 - Si ha seleccionado **Discover Unassigned Server (Descubrir mediante una dirección IP)**, proporcione la dirección IP del servidor que desea descubrir.
 - Si ha seleccionado **Descubrir mediante un rango IP**, proporcione el rango de direcciones IP que desea incluir y si debe excluir un rango de direcciones IP, seleccione **Habilitar rango de exclusión** y proporcione el rango que desea excluir.
5. Introduzca un nombre de tarea exclusivo y, a continuación, haga clic en **Finalizar**.
6. (Opcional) Seleccione la opción **Ir a la lista de trabajos** para realizar un seguimiento de esta tarea.
Se muestra la página **Centro de trabajos y registros**. En la pestaña **En ejecución**, expanda el trabajo de detección para ver el progreso de este trabajo.

Eliminación de servidores de la consola de DLCI

Puede eliminar los servidores sin asignar y los servidores del host según los siguientes criterios:

- Puede eliminar un servidor sin asignar que se indica en el servidor.
- Si se aprovisiona un servidor de host en SCVMM y está presente en el servidor, primero debe eliminar el servidor en SCVMM y, a continuación, eliminar el servidor del servidor.

En la consola de DLCI:

- Para eliminar servidores sin asignar: en **Servidores sin asignar**, seleccione el servidor y haga clic en **Eliminar**. En el mensaje de confirmación, haga clic en **Sí**.
- Para eliminar servidores de host: en **Servidores de host**, seleccione el servidor y haga clic en **Eliminar**. En el mensaje de confirmación, haga clic en **Sí**.

Visualización de inventario del dispositivo

En la página **Inventario del dispositivo** se muestran los servidores sin asignar y los servidores del host. Utilizando el nombre de host o la dirección IP del servidor, puede ver los detalles del servidor, como el estado de cumplimiento de normas, las versiones de firmware, etc.

En la página Inventario de dispositivos, puede hacer lo siguiente:

- [Detección de servidores](#)
- Actualizar información del servidor
- [Eliminación de servidores de la consola de DLCI](#)
- [Sincronización con SCVMM](#)
- [Resolución de errores de sincronización](#)
- Correlacionar servidores del host con un grupo de clúster y el chasis al que pertenece el servidor

- [Inicio de la consola de iDRAC](#)

Si el servidor sin asignar es un servidor modular, la etiqueta de servicio del chasis se agrega a los detalles de inventario del chasis que contiene el servidor modular.

Si el servidor del host es parte de clúster, para correlacionar un servidor con su grupo de clústeres y para conocer la información del chasis, consulte FGDN de clúster y etiqueta de servicio del chasis.

Para trabajar con los servidores descubiertos en versiones anteriores del servidor, vuelva a descubrir los servidores.

Para ver los servidores:

En la consola de DLCI, haga clic en **Inventario de dispositivo**.

Sincronización con SCVMM

Con el dispositivo, puede sincronizar todos los hosts de Hyper-V, los clústeres de hosts Hyper-V y los hosts Hyper-V modulares de Dell en el entorno SCVMM. También puede obtener el inventario más reciente del firmware de los servidores tras la sincronización.

Notas sobre sincronización:

- La sincronización utiliza los detalles del perfil de credenciales del iDRAC predeterminados de los servidores.
- Si la controladora de administración de tarjeta madre (BMC) del servidor host no está configurada con la dirección IP de iDRAC en SCVMM, entonces no puede sincronizar el servidor host con el dispositivo. Por lo tanto, configure BMC en SCVMM (para obtener más información, consulte el artículo de MSDN en technet.microsoft.com) y, luego, sincronice el dispositivo con SCVMM.
- En SCVMM R2, varios hosts en el entorno están soportados y, por este motivo, la sincronización es una tarea de ejecución larga. La sincronización se realiza de la siguiente manera:
 1. Los hosts que se enumeran en el entorno de SCVMM se agregan a la pestaña **Hosts** del dispositivo.
 2. Durante la resincronización, los servidores host que se eliminaron del entorno SCVMM se transfieren a la pestaña **Sin asignar** en el dispositivo. Si un servidor quedó fuera de servicio, entonces elimine ese servidor de la lista de servidores sin asignar.
 3. Si el servidor aparece como un servidor sin asignar y agregado manualmente a SCVMM, después de la sincronización el servidor se agrega a la pestaña **hosts** del appliance.
 4. Si un servidor host pertenece a un clúster Hyper-V, los detalles del clúster estarán disponibles en el inventario del dispositivo. El servidor host se agrega o se transfiere al grupo de actualización de clúster.
 5. Si un host es un servidor modular, la etiqueta de servicio del chasis que contiene el servidor modular se agrega a la página de inventario del dispositivo. Si el servidor modular no pertenece a un clúster Hyper-V, el servidor host se agrega o se mueve al grupo de actualización del chasis.
 6. Los cambios que se realicen en los detalles de inventario de host como, por ejemplo, el nombre de host, la dirección IP del iDRAC, la memoria, la pertenencia al clúster, etc. se actualizan en el inventario de dispositivos.
 7. DLCI para SCVMM puede proporcionar la información de inventario del firmware más reciente. Si se proporciona una fuente de actualización predeterminada, el inventario del firmware se compara con la fuente de actualización y la información más reciente se agrega al grupo de actualización.

Sincronización del servidor con SCVMM

Para realizar la sincronización:

En **DLCI para SCVMM**, haga clic en **Inventario de dispositivo** y, a continuación, haga clic en **Sincronizar con SCVMM**.

Resolución de errores de sincronización

Los servidores que no están sincronizados con el servidor se enumeran con su dirección IP y nombre de host del iDRAC.

Tenga en cuenta lo siguiente al resolver errores de sincronización:

- En el caso de servidores que no están sincronizados debido a las credenciales, el iDRAC, la conectividad u otros problemas; resuelva los problemas en primer lugar, y, a continuación, vuelva a sincronizar.

Para sincronizar los servidores:


1. En Complemento de la consola de DLCI para SCVMM, haga clic en **Inventario de dispositivos** y, a continuación, haga clic en **Resolver errores de sincronización**.

2. Seleccione los servidores que desea sincronizar y seleccione el perfil de credenciales o cree un perfil de credenciales nuevo.
3. Proporcione un nombre para el trabajo y, a continuación, haga clic en **Finalizar**.
4. (Opcional) Seleccione la opción **Go to the Job List (Ir a la lista de trabajos)** para ver el estado de la tarea automáticamente una vez que se envíe la tarea.

Inicio de la consola de iDRAC

Para iniciar la consola de iDRAC:

En **Inventario de dispositivos**, bajo **Servidores sin asignar** o **Hosts**, haga clic en **IP de iDRAC**.

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

Licencia para el appliance

Las funciones en DLCI para SCVMM de configuración sin agente, implementación del sistema operativo, actualización del firmware, reemplazo de partes y exportación e importación del perfil de servidor tienen licencia. Hay cinco licencias disponibles para fines de evaluación sin cargo adicional. Para descargar las cinco licencias, consulte marketing.dell.com/software-download-DLCISCVMM. Para obtener más información sobre el licenciamiento, vaya al sitio web de Dell TechCenter y luego a la página Wiki de OpenManage Integration Suite para Microsoft System Center.

Para ver los detalles de la licencia, en **Portal de administración de DLCI - SCVMM**, inicie el **Centro de licencias**.

Administración del servidor

Mediante el **Centro de mantenimiento**, puede realizar todas las tareas relacionadas con la administración de las actualizaciones de Dell en el entorno SCVMM. Puede mantener actualizadas las versiones del firmware de los componentes del servidor de Dell según las recomendaciones de Dell.

Puede ver, crear y mantener los vaults de protección, las fuentes de actualización, los grupos personalizados y ver los grupos de actualización predefinidos. Puede crear y programar trabajos para las actualizaciones del firmware, como también programar notificaciones para recibir alertas cuando haya catálogos nuevos disponibles en la fuente de actualización. Se proporciona un informe de comparación para la versión de firmware existente y la versión base, y, según esta información, puede crear un archivo de inventario e importar y exportar perfiles de servidor. Además, puede filtrar la información según el tipo de actualizaciones y los componentes y modelos del servidor.

Puede realizar las actualizaciones solo en los servidores compatibles, ya que las actualizaciones del iDRAC están disponibles solo para la versión compatible mínima y posteriores.

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

DLCI para SCVMM proporciona las siguientes acciones de actualización:

- Degradación: existe una versión anterior disponible en un origen de actualización y puede degradar el firmware a esta versión.
- No se requiere ninguna acción: la versión del firmware está en el mismo nivel que la del repositorio.
- No hay actualizaciones disponibles: no hay actualizaciones de firmware disponibles para el componente.
- Actualización (opcional): las actualizaciones constan de funciones nuevas o de actualizaciones de configuración específicas que son opcionales.
- Actualización (urgente): las actualizaciones críticas utilizadas para resolver situaciones críticas de seguridad, rendimiento o reparación de errores en componentes como BIOS, etc. están disponibles.
- Actualización (recomendada): las actualizaciones incluyen correcciones de errores o mejoras de función en el producto. Además, se incluyen correcciones de compatibilidad con otras actualizaciones de firmware.

DLCI para SCVMM proporciona los siguientes métodos para realizar las actualizaciones de firmware:

- **Actualización mediante repositorio de DRM** : exporte la información de inventario de los servidores descubiertos desde un servidor para preparar un repositorio en DRM. Para obtener información sobre cómo exportar la información de inventario, consulte [Exportación del inventario](#).
 - Después de crear el repositorio en DRM, seleccione los servidores pertinentes e inicie una actualización en los servidores. Tenga en cuenta otros factores como el entorno de pruebas, las actualizaciones de seguridad, las recomendaciones de aplicación, las asesorías de Dell y más para preparar las actualizaciones necesarias. Para obtener más información acerca de la creación de un repositorio, consulte los documentos de *Dell Repository Manager* disponibles en dell.com/support/home.
- **Actualización mediante FTP o HTTP**: actualice cualquier componente específico a la versión más reciente que se proporciona en el sitio FTP o HTTP. Dell IT prepara un repositorio de forma trimestral.
 - Integración con el catálogo en línea de Dell: conecte con el FTP de Dell y descargue el archivo de catálogo del directorio de memoria caché en caso de origen de actualización FTP, o conecte con `downloads.dell.com` en caso de fuente de actualización HTTP y, a continuación, conviértalo en inventario de referencia.
 - Vea el informe de comparación con el origen de actualizaciones, seleccione los servidores o componentes del servidor relevantes y, a continuación, inicie la actualización en los servidores.
- **Inventario del firmware de referencia y comparación**: cree un archivo de inventario de referencia que contenga el inventario del firmware de los servidores o grupos de servidores seleccionados. Luego, puede comparar la información de inventario de los servidores presentes en el dispositivo con el archivo de inventario de referencia guardado. Cabe señalar que el archivo de inventario de referencia del servidor puede contener información de inventario de un solo servidor del mismo tipo o modelo, o bien puede tener varios servidores de diferentes tipos o modelos.

Temas:

- [Integración con DRM](#)

- Filtros
- Descripción general de origen de actualización
- Grupos de actualización
- Aplicación de actualizaciones en servidores
- Sondeo y notificación
- Almacén de protección
- Sustitución de piezas
- Recopilación de registros del controlador Lifecycle
- Exportación de inventario
- Exportación de perfiles de servidor
- Importación del perfil del servidor
- Administrar los trabajos

Integración con DRM

DLCI para SCVMM se integra con DRM versión 2.2 y posteriores, lo que proporciona la información del inventario del servidor de los servidores existentes desde el dispositivo hasta DRM. Al usar la información de inventario, puede crear un repositorio personalizado en DRM y configurarlo como una fuente de actualización en el dispositivo para realizar trabajos de actualización del firmware en los servidores o en un grupo de servidores. Para obtener más información sobre la creación de un repositorio en DRM, consulte los documentos de *Dell Repository Manager*.

NOTA: Después de actualizar a la versión 1.2 de DLCI para SCVMM, realice una nueva detección de los servidores para actualizar la información de inventario consumida por DRM.

Para crear un repositorio para el appliance mediante DRM:

1. Abra la versión de **Dell Repository Manager Data Center**.
2. Haga clic en **Mis repositorios**, haga clic en **Nuevo** y, a continuación, haga clic en **Integración de la consola Dell**.
3. Escriba la **URL (API de Rest)** en el siguiente formato: `https:// IP address of appliance/genericconsolerepository/` . Luego, haga clic en **Siguiente**.
4. Proporcione el **Nombre de usuario** y la **Contraseña** que se utilizaron en el servidor, haga clic en **Aceptar** y, a continuación, haga clic en **Aceptar**

Filtros

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

El servidor es compatible con 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 filtros:

En el complemento de consola de DLCI, haga clic en **Centro de mantenimiento**, haga clic en el menú desplegable de filtros y, a continuación, seleccione los filtros.

Para quitar los filtros:

En el complemento de consola de DLCI, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Borrar filtros** o anule la selección de las casillas seleccionadas.

Descripción general de origen de actualización

La fuente de actualización le permite seleccionar y aplicar las actualizaciones de las fuentes de actualización de Dell. Puede crear, ver y administrar las fuentes de actualización. FTP, HTTP y repositorio DRM son los tipos de fuentes de actualización soportados. Puede crear una fuente de actualización DRM, HTTP o FTP y configurarla como una fuente de actualización predeterminada.

Las fuentes de actualización incluyen los archivos de catálogo que contienen actualizaciones de Dell (BIOS, firmware, aplicación, controladores y paquetes de controladores) e incluyen los archivos ejecutables autocontenidos denominados Dell Update Packages (DUP).

Una copia local del archivo del catálogo se almacena en la memoria caché del dispositivo en el momento de la creación. 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 o elimine la fuente de actualización y vuelva a crear la fuente de actualización.

Puede comparar la información del inventario disponible en la fuente de actualización con la información de inventario de un servidor o grupo de servidores seleccionado y crear una versión base. También puede cambiar la fuente de actualización y comparar la información del inventario de los servidores o grupos de servidores con la información de la versión disponible en la fuente de actualización seleccionada.

En Dell se recomienda actualizar al firmware más reciente para aprovechar la seguridad, las correcciones de errores y las solicitudes de funciones nuevas. En Dell se publican las siguientes actualizaciones a través de los catálogos PDK publicados en Dell FTP de manera trimestral:

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

Origen de actualización predefinido y predeterminado

El **CATÁLOGO EN LÍNEA DE DELL** es una fuente de actualización predefinida de tipo FTP disponible en el dispositivo después de una nueva instalación o actualización. No puede eliminar o cambiar el nombre de una fuente de actualización predefinida.

El **CATÁLOGO HTTP EN LÍNEA DE DELL** es una fuente de actualización predeterminada disponible en el dispositivo después de una nueva instalación o actualización. No puede eliminar ni cambiar el nombre de esta fuente de actualización predeterminada. Sin embargo, puede crear otro origen de actualización y marcarlo como un origen de actualización predeterminado.

NOTA:

- Después de instalar DLCI para SCVMM, introduzca los detalles del proxy para la fuente de actualización del **CATÁLOGO EN LÍNEA DE DELL** y el **CATÁLOGO DE HTTP EN LÍNEA DE DELL** y guárdelo.
- Después de actualizar a la versión 1.2 de DLCI para SCVMM, establezca **DELL ONLINE HTTP CATALOG (CATÁLOGO HTTP EN LÍNEA DE DELL)** como fuente de actualización predeterminada.

Probar conexión

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

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

Configuración de FTP local

Para configurar el FTP local:

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

Configuración de HTTP local

Para configurar el servidor HTTP en un sistema local, realice lo siguiente:

1. Cree una estructura de carpetas en el HTTP local que sea una réplica exacta de `downloads.dell.com`.
2. Descargue el archivo `catalog.xml.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** a la URL del HTTP local y, luego, comprima el archivo con la extensión `.gz`.
Por ejemplo, cambie la **Ubicación base** de `downloads.dell.com` a `hostname.com`.

4. Coloque el archivo de catálogo con el archivo de catálogo modificado y los archivos DUP en su carpeta HTTP local replicando la misma estructura de `downloads.dell.com`.

Visualización del origen de actualizaciones

Para ver un origen de actualizaciones:

1. En **DLCI para SCVMM**, 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**.

Creación de un origen de actualizaciones

Requisitos previos:

- Según el tipo de origen de actualizaciones, se necesita un perfil de credenciales de Windows o FTP.
- Si va a crear un origen de actualizaciones de DRM, asegúrese de que DRM esté instalado y de que los roles de Administrador estén configurados.

Para crear un origen de actualizaciones:

1. En **Complemento de consola de DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Configuración de mantenimiento**.
2. En **Origen de actualizaciones**, haga clic en **Crear nuevo** y proporcione la información necesaria.
 - 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.
 - 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 de ubicación, ingrese la ruta completa del archivo de catálogo con el nombre del archivo.
3. (Opcional) Para que sea el origen de actualizaciones predeterminado, seleccione **Hacer que sea el origen predeterminado**.
4. Haga clic en **Probar la conexión** para verificar la ubicación del origen de actualización y, a continuación, haga clic en **Guardar**.

 **NOTA:** Utilice solo DUP de 32 bits para crear el origen de actualización en DRM.

 **NOTA:** Una vez verificada la ubicación, puede crear el origen de actualización.

Modificación del origen de actualizaciones

Tenga en cuenta lo siguiente al modificar un origen de actualizaciones:

- 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 continuar con los cambios.

Para modificar un origen de actualizaciones:

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

Eliminación de origen de actualizaciones

No puede eliminar un origen de actualizaciones en las siguientes circunstancias:

- El origen de actualización es un origen de actualización predefinido: **Dell Online Catalog (Catálogo en línea de Dell)** y **DELL ONLINE HTTP CATALOG (CATÁLOGO HTTP EN LÍNEA DE DELL)**.
- El origen de actualizaciones se utiliza en una plantilla de implementación.
- Un trabajo en curso o programado utiliza el origen de actualización.
- El origen de actualizaciones es un origen de actualizaciones predeterminado.

Para eliminar un origen de actualizaciones:

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

Grupos de actualización

Los grupos de actualización son un grupo de servidores que requieren una administración de actualizaciones similar. Hay dos tipos de grupos de actualización disponibles, predefinidos y personalizados. Puede ver los grupos predefinidos. Sin embargo, puede crear y mantener los grupos de actualización personalizados.

NOTA: Después de actualizar la versión 1.1 de DLCI para SCVMM a la versión 1.2, todos los servidores descubiertos anteriormente se agregan a los **Grupos de actualización genéricos** o a los **Grupos de actualización de hosts**. Para agregar los servidores a los respectivos grupos de actualización predefinidos, vuelva a descubrir los servidores.

Grupos de actualización predefinidos

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

- **Grupos de actualización genéricos**
 - **Todos los grupos de actualización**
 - **Grupos de actualización de servidor sin asignar predeterminados**
- **Grupos de actualización de clúster**
- **Grupos de actualización de host**
 - **Grupos de actualización de host predeterminados**
- **Grupos de actualización del chasis**

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

Todos los grupos de actualización: este grupo consta de todos los grupos de servidores. Cualquier grupo presente en el dispositivo es miembro de todos los grupos de actualización. Este grupo es del tipo de grupo de actualización genérico.

Grupo de actualización de servidor predeterminado sin asignar: este grupo consta de todos los servidores sin asignar que no forman parte de ningún otro grupo. Este grupo es del tipo de grupo de actualización genérico. Los servidores se agregan al grupo de actualización de servidor predeterminado sin asignar después de:

- un descubrimiento nuevo o un redescubrimiento de servidores físicos (bare metal).
- una sincronización o resincronización, después de eliminarlo de SCVMM pero aún presente en el servidor.

Grupo de actualización de clúster: este grupo consta de clústeres de conmutación por error de Windows Server. Si un servidor modular pertenece a un clúster, se agrega al grupo de actualización de clúster. Si un servidor modular de 12.^a o 13.^a generación de Dell PowerEdge es parte de un clúster, entonces también se agrega la información de CMC en el inventario de la página **Centro de mantenimiento**.

Para conocer el grupo de actualización de clúster al que pertenece el servidor, consulte la página de inventario del dispositivo donde se muestra el nombre de host y el FQDN de clúster de todos los servidores mostrados en el servidor.

Host update group (Grupo de actualización de host): este grupo consta de servidores de host y las actualizaciones se aplican en una sola sesión que se refiere a la actualización de todos los servidores del grupo a la vez.

Grupo de actualización de host predeterminado: este grupo consta de todos los hosts descubiertos que no forman parte de ningún otro grupo de actualización. Este grupo es del tipo de grupo de actualización de host.

Grupo de actualización del chasis: los servidores modulares que pertenecen a un chasis y que no forman parte de ningún grupo de clústeres se clasifican en este grupo. Los servidores de 12.^a o 13.^a generación de Dell PowerEdge se descubren junto con su información de CMC. De forma predeterminada, un grupo se crea con el formato de nomenclatura `Chassis-Service-tag-of-Chassis-Group` 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 personalizado

Puede crear, modificar y eliminar los grupos de actualización personalizados. Sin embargo, solo puede agregar un servidor a un grupo de actualización personalizado desde **Grupos de actualización predeterminados sin asignar** y **Grupos de actualización de host predeterminados**. Después de agregar un servidor a un grupo de actualización personalizado, se elimina el servidor del grupo de

actualización predefinido y solo estará disponible en el grupo de actualización personalizado. Para agregar los servidores a un grupo de actualización personalizado, busque los servidores mediante su etiqueta de servicio.

Métodos de actualización

Puede aplicar las actualizaciones seleccionadas a grupos de servidores seleccionados que sean compatibles.

- Puede realizar las siguientes actualizaciones en los grupos de servidores:
 - **Actualizaciones en etapas sin agente:** se refiere a las etapas de actualizaciones del firmware. Las actualizaciones del firmware que se pueden aplicar de inmediato y que no requieren un reinicio se aplican inmediatamente. Las actualizaciones restantes que requieran un reinicio del sistema se aplican al reiniciar del servidor. Las actualizaciones se realizan en lotes a la hora programada mediante iDRAC. El tamaño del lote se determina cuando se está realizando la actualización. Actualice el inventario para comprobar si se aplicaron todas las actualizaciones. Si la operación falla incluso en solo un servidor, todo el trabajo de actualización fallará.
 - **Actualizaciones sin agente:** se trata de la actualización fuera de banda con reinicio inmediato del servidor.
 - **Actualización compatible con clústeres (CAU):** automatiza el proceso de actualización al aprovechar la función CAU de Windows en grupos de actualización de clúster para mantener la disponibilidad del servidor. Las actualizaciones en los servidores se realizan a través del coordinador de actualización de clúster, que está presente en el mismo sistema en el que está instalada la Gateway de integración (IG) y no a través de iDRAC. Las actualizaciones no ocurren por etapas y se aplican de inmediato. Mediante la 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 Visión general de la actualización compatible con clústeres en technet.microsoft.com.

Notas de grupos de actualización

- No puede crear, modificar ni eliminar los grupos de actualización predefinidos manualmente.
- No puede actualizar el firmware de la CMC directamente desde el servidor. Sin embargo, puede actualizar el firmware del servidor modular presente en la CMC. Para actualizar el firmware de la CMC, consulte Actualización del firmware de la CMC en la *Guía del usuario de Dell PowerEdge M1000e Chassis Management Controller Firmware*. Para actualizar el firmware de la CMC en VRTX, consulte Actualización del firmware en la *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide (Guía del usuario de Dell Chassis Management Controller para Dell PowerEdge VRTX)* y para actualizar el firmware de la CMC en FX2, consulte Actualización del firmware en la *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide (Guía del usuario de Dell Chassis Management Controller para Dell PowerEdge FX2)*.

Visualización grupos de actualización

Para ver grupos de actualización:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Configuración de mantenimiento**.
2. En **Configuración de mantenimiento**, haga clic en **Actualizar grupos**.

Creación de grupos actualización personalizados

Para crear grupos de actualización personalizados:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic 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. Proporcione los detalles y seleccione el tipo de grupo de actualización que desee crear.

Los grupos de actualización personalizados pueden tener servidores solamente de los siguientes tipos de grupos de actualización:

 - Grupo de actualización de host genérico: se compone de servidores de los grupos de actualización sin asignar predeterminados y de grupos de actualización de host.
 - Grupo de actualización de host: se compone de servidores de grupos de actualización de host predeterminados.
4. Para agregar servidores al grupo de actualización, busque los servidores mediante su etiqueta de servicio, y haga clic en **Guardar**.

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:
 - Elimine el servidor del grupo de actualización personalizado existente. Así se agrega automáticamente en el grupo de actualización predefinido.
 - Ahora edite el grupo personalizado para agregarle el servidor y, a continuación, busque el servidor mediante la etiqueta de servicio.

Para modificar un grupo de actualización personalizado:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic 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 **Editar** para modificar el grupo de actualización.

Eliminación de grupos actualización personalizados

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

- No puede eliminar un grupo de actualización si dispone de un trabajo programado, en curso o a la espera.
- Puede eliminar un grupo de actualización, incluso si los servidores están presentes en dicho grupo de actualización. Sin embargo, después de eliminar ese grupo de actualización, los servidores se mueven a sus respectivos grupos de actualización predefinidos.

Para eliminar un grupo de actualización personalizado:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic 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.

Aplicación de actualizaciones en servidores

Puede aplicar actualizaciones inmediatas o programar las actualizaciones en servidores o en un grupo de servidores mediante la creación de trabajos de actualización de firmware. Los trabajos creados para actualizaciones aparecen en la página **Centro de trabajos y registros**. Además, puede volver a la versión anterior sugerida del firmware seleccionando **Permitir degradación**. Si esta opción no está seleccionada, entonces no hay una acción en el componente que exija una degradación de firmware.

NOTA:

- Puede aplicar las actualizaciones de firmware a un único componente de un servidor, o a todo el entorno.
- Si no hay actualizaciones o degradaciones aplicables para un servidor o grupo de servidores, si realiza una actualización de firmware en dicho servidor o grupo de servidores, no se produce ninguna acción en los mismos.
- Cuando actualiza información a nivel de componentes, si la versión del firmware existente es igual a la versión del firmware del origen de actualización, no se producirá ninguna acción en dicho componente.

Requisitos previos:

- Para actualizar servidores, necesita contar con una fuente de actualización en un sitio FTP de Dell, un sitio FTP local, HTTP, o Dell Repository Manager (DRM).
- Antes de aplicar las actualizaciones, deje en blanco la cola de trabajos del iDRAC donde se aplican las actualizaciones.
- Asegúrese de que el usuario de IG tiene privilegios de administrador local en todos los nodos del clúster.
- Antes de aplicar las actualizaciones en grupos de actualización de clúster, active el informe de disponibilidad del clúster para lo siguiente:
 - La conectividad con origen de actualización.
 - La disponibilidad de los clústeres de conmutación por error.
 - Asegúrese de que el sistema operativo Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016 esté instalado en todos los nodos del clúster de conmutación por error para admitir la función CAU.
 - La configuración de las actualizaciones automáticas no está habilitada para instalar automáticamente actualizaciones en cualquier nodo del clúster de conmutación por error.
 - La activación de una regla de servidor de seguridad que permita el apagado remoto en cada nodo del clúster de conmutación por error.

- Valide las opciones de ejecución de actualización configuradas. Para obtener más información, consulte la sección Requisitos y prácticas recomendadas para el clúster: actualización compatible en technet.microsoft.com.
- El grupo de clústeres debe tener un mínimo de dos nodos.
- Compruebe la preparación para la actualización del clúster. Para obtener más información acerca de CAU, consulte la sección Requisitos y prácticas recomendadas para el clúster: actualización compatible en technet.microsoft.com.

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

Para aplicar las actualizaciones en servidores:

1. En el complemento de consola de DLCI para SCVMM, haga clic en **Centro de mantenimiento**, seleccione el servidor o el grupo de servidores y una fuente de actualizaciones, y, a continuación, haga clic en **Ejecutar actualización**.

NOTA:

- Para una actualización a nivel de componentes, expanda los grupos de servidores a su nivel de componentes y haga clic en **Ejecutar actualización**.
- Cuando se realiza una actualización de firmware para la 11.ª generación de servidores Dell PowerEdge, no puede actualizar las versiones de firmware de la unidad de suministro de energía (PSU).

2. En **Detalles de la actualización**, proporcione el nombre y la descripción del trabajo de actualización de firmware.

3. En **Programar actualización**, seleccione una de las opciones siguientes:

- **Run Now (Ejecutar ahora):** para aplicar las actualizaciones ahora.
- Seleccione la fecha y la hora para programar una actualización de firmware en el futuro.

4. Seleccione el método de la actualización mediante **Actualización sin agente** o **Actualización sin agente en etapas** y, a continuación, haga clic en **Terminar**.

NOTA: Después de enviar un trabajo de actualización de firmware a iDRAC, el dispositivo interactúa con iDRAC para solicitar el estado del trabajo y proporciona actualizaciones de estado en la página **Trabajos y registros** en la consola de administración. En ocasiones, iDRAC no proporciona actualizaciones de estado en los trabajos que el dispositivo rastrea. El dispositivo espera un máximo de 6 horas y, si no hay respuesta desde iDRAC, el estado del trabajo de actualización del firmware se considera fallido.

Sondeo y notificación

Puede recibir notificaciones cuando estén disponibles nuevos catálogos durante la generación del sistema y los orígenes de actualización predeterminados.

El color de la campana de notificación cambia a color naranja cuando hay un nuevo archivo de catálogo disponible en la fuente de actualización. Haga clic en el icono de campana para reemplazar el catálogo en caché local disponible en la fuente de actualización. Una vez que los catálogos antiguos se reemplazan por los más recientes, el color de la campana cambia a verde.

Configuración de notificaciones

Para configurar la frecuencia de sondeo:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento**, luego en **Configuración de mantenimiento** y, a continuación, haga clic en **Sondeo y notificación**.
2. Seleccione la frecuencia a la que se llevará a cabo el sondeo:
 - **Nunca:** esta opción está seleccionada de manera predeterminada. Seleccione para recibir actualizaciones sobre nuevos catálogos disponibles en la fuente de actualización solo una vez durante la hora programada.
 - **Una vez a la semana:** seleccione esta opción para recibir actualizaciones sobre nuevos catálogos disponibles en el origen de actualización semanalmente.
 - **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.

Almacén de protección

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

Creación del almacén de protección

Requisitos previos: asegúrese de que se puede acceder a la ubicación del almacén.

Para crear un almacén de protección:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Configuración de mantenimiento**.
2. En **Centro de mantenimiento**, haga clic en **Centro de protección** y, a continuación, haga clic en **Crear**.
3. Seleccione el tipo de almacén de protección que desea utilizar y proporcione los detalles necesarios.
 - Si está creando un vault de protección del tipo de **Recurso compartido de red**, introduzca la ubicación para guardar los perfiles, las credenciales para acceder a esta ubicación y una frase de contraseña para asegurar el perfil. Este tipo de vault de protección proporciona soporte para el uso compartido de archivos de tipo Sistema de archivos de Internet comunes (CIFS, por sus siglas en inglés).
 - 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

Tenga en cuenta lo siguiente al modificar un almacén de protección:

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

Para modificar un almacén de protección:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Configuración de mantenimiento**.
2. En **Centro de mantenimiento**, haga clic en **Almacén de protección** y, a continuación, haga clic en **Editar** para modificar el almacén.

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.
 - Hay un trabajo programado que está asociado con almacén de protección. Sin embargo, para eliminar dicho vault de protección, elimine el trabajo programado y, a continuación, elimine el vault de protección.
1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Configuración de mantenimiento**.
 2. En **Centro de mantenimiento**, haga clic en **Almacén de protección** y, a continuación, haga clic en **Eliminar** para eliminar el almacén.

Sustitución de piezas

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

Se admiten las siguientes opciones:

- 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.
- Part firmware update (Actualización del firmware de las piezas): restaura, actualiza o degrada la versión de firmware de los componentes en función de la selección.

- **Disabled (Desactivado):** la función está desactivada se aplica lo mismo a la pieza sustituida.
- **Allow version upgrade only (Permitir solo la actualización de la versión):** las versiones de firmware actualizadas se aplican en los componentes sustituidos, si la versión de firmware de la pieza nueva es anterior a la versión existente.
- **Match firmware of replaced part (Coincidencia de firmware de la pieza reemplazada):** la versión de firmware del componente nuevo se coincide con la versión de firmware del componente original.
- **No cambiar el valor en el servidor:** se conserva la configuración actual del componente.
- Part configuration update (Actualización de la configuración de las piezas): restaura o actualiza la configuración de los componentes según lo que se seleccione.
 - Disabled (Desactivado): la función está desactivada y la configuración guardada del antiguo componente no se aplica al componente sustituido.
 - **Apply always Aplicar siempre:** la función está activada y la configuración guardada del antiguo componente se aplica al componente sustituido.
 - **Apply only if firmware matches (Aplicar solo si coincide el firmware):** la configuración guardada del antiguo componente se aplica a los componentes sustituidos solo si sus versiones de firmware coinciden.
 - **No cambiar el valor en el servidor:** se conserva la configuración existente.

Aplicar el firmware y los valores de configuración

Para establecer los parámetros para sustitución de piezas:

1. En **Complemento de la consola de DLCI para SCVMM**, en **Centro de mantenimiento** seleccione los servidores o grupo de servidores y, a continuación, haga clic en **Configurar sustitución de piezas**. Se muestra la ventana **Configure Part Replacement (Configurar reemplazo de piezas)**.
2. Establezca los valores de **CSIOR**, **Actualización de firmware de las piezas** y **Actualización de la configuración de las piezas** y, a continuación, haga clic en **Finalizar**.

Recopilación de registros del controlador Lifecycle

Los registros de LC proporcionan registros de actividades pasadas en un sistema 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 que ofrecen los registros de LC: alertas relacionadas con los cambios de configuración en los componentes de hardware del sistema, cambios del firmware debidos a una actualización de la versión o regreso a una versión anterior, piezas reemplazadas, advertencias sobre la temperatura, fecha y hora detalladas del momento en el que se inició la actividad, gravedad de la actividad, etc.

Existen dos opciones para recopilar registros de LC:

- Registros de LC activos: estos son los archivos de registro de LC recientes. Puede ver, buscar y exportar estos archivos de registro al dispositivo. Puede programar un trabajo para recopilar los registros de LC en el dispositivo o en un recurso compartido de red. Además, puede guardar un respaldo del archivo de registro en un recurso compartido de red.
- Registros de LC completos: estos registros contienen archivos de registro de LC activos y archivados. Son de gran tamaño, por lo que están comprimidos en el formato .gz y se exportan a la ubicación especificada en un recurso compartido de red CIFS.

Recopilar registros de LC

1. En **Complemento de la consola de DLCI para SCVMM**, en **Centro de mantenimiento** seleccione un servidor o en un grupo de servidores y, a continuación, haga clic en **Recopilar registros de LC**.
2. En **Recopilación de registros de LC**, seleccione una de las opciones siguientes y haga clic en **Finalizar**.
 - **Export Complete LC Logs (.gz) (Exportar registros de LC completos [.gz]):** exporta los registros de LC activos y archivados a un recurso compartido de red CIFS proporcionando las credenciales de Windows.

NOTA:

- Asegúrese de que la carpeta compartida tiene espacio suficiente para guardar los registros de LC completos, ya que estos son archivos de gran tamaño.
- Exportar registros de LC completos no se admite con servidores Dell PowerEdge de 11.ª generación.
- Los registros de LC se guardan en el siguiente 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.

- **Exportar registros activos (Ejecutar ahora):** seleccione esta opción para exportar los registros activos inmediatamente al dispositivo.
 - (Opcional) Habilite la opción **Back up LC logs on the network share (Realizar copias de seguridad de los registros de LC en el recurso compartido de red)** para guardar una copia de seguridad de los registros de LC en el recurso compartido de red CIFS proporcionando las credenciales de Windows.
- **Recopilación de registros de LC programados:** seleccione una fecha, hora y frecuencia para exportar los registros de LC activos.
 - (Opcional) Habilite la opción **Back up LC logs on the network share (Realizar copias de seguridad de los registros de LC en el recurso compartido de red)** para guardar una copia de seguridad de los registros de LC en el recurso compartido de red CIFS proporcionando las credenciales de Windows.

NOTA: Asegúrese de actualizar a las versiones más recientes del iDRAC y active LC antes de exportar registros de LC para servidores Dell PowerEdge de 11.^a.

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

- **Nunca:** seleccione esta opción para exportar el perfil de servidor solo una vez durante 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.

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

Ver registros de LC

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

1. En **Complemento de la consola de DLCI para SCVMM**, en **Centro de mantenimiento** seleccione un servidor o en un grupo de servidores y, a continuación, haga clic en **Ver registros de LC**. 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.
2. Haga clic en el nombre de archivo para ver todas las entradas de registro del archivo de registro de LC específico de ese servidor.
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 archivo LC:

- Haga clic en el nombre de archivo para abrir el archivo de registro de LC y busque una descripción en el cuadro de búsqueda.
- Introduzca una descripción en el cuadro de búsqueda y, a continuación, vea todos los archivos de LC con las instancias de la siguiente descripción.

NOTA:

- Si la descripción del mensaje del registro de LC es larga, el mensaje se truncará a 80 caracteres.
- El tiempo que se muestra comparando los mensajes de registro de LC sigue la zona horaria del iDRAC.
- Antes de descargar los registros de LC, agregue el dispositivo en el sitio Intranet local.

Para agregar el dispositivo al sitio **Intranet local**:

- a. Abra **Internet Explorer**, haga clic en **Herramientas** y, a continuación, haga clic en **Opciones de Internet**.
- b. Haga clic en **Seguridad**, seleccione **Intranet local** y, a continuación, haga clic en **Sitios**. Aparecerá la página **Intranet local**.
- c. Haga clic en **Avanzado**, escriba la URL del dispositivo, y haga clic en **Agregar**.

Exportación de inventario

En DLCI para SCVMM, puede exportar el inventario de los 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. También puede importar el archivo XML en DRM, crear un repositorio basado en el archivo de inventario y crear una configuración de referencia.

Para exportar un inventario de firmware de los servidores o los grupos de servidores al utilizar Internet Explorer versión 10 y posteriores, agregue la dirección IP del complemento de consola al sitio de **Intranet local**. Antes de exportar el archivo de inventario, realice los siguientes pasos:

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

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

Para exportar el inventario de servidores detectados:

1. En **Complemento de consola de DLCI para SCVMM**, 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**.

NOTA: Para crear un repositorio de DRM después de exportar el archivo XML, realice lo siguiente:

1. Haga clic en **Mis repositorios, Nuevo** y, a continuación, haga clic en **Inventario de chasis modular de Dell**.
2. Introduzca un nombre y una descripción en la sección **Repositorio base** y haga clic en **Siguiente**.
3. Haga clic en **Buscar** para seleccionar el archivo del inventario exportado del dispositivo en la sección **Inventario de chasis modular** y, a continuación, haga clic en **Siguiente**. Para obtener más información acerca de la creación de un repositorio, consulte los documentos de *Dell Repository Manager* disponibles en dell.com/support/home.

Visualización y actualización de inventario de firmware

Puede ver y actualizar el inventario de firmware de los servidores compatibles con Dell después de seleccionar un servidor o un grupo específico de servidores.

Puede ver el informe de comparación del inventario del servidor o del chasis en contraste con una fuente de actualización seleccionada. Puede cambiar la fuente de actualización y ver el informe de comparación de la información del inventario de los servidores, los grupos de servidores o el chasis seleccionados en función de la fuente de actualización modificada.

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

NOTA:

- La versión 1.2 de DLCI para SCVMM incluye un catálogo que muestra una versión anterior del informe de comparación para la fuente de actualización predefinida de FTP y HTTP. Por lo tanto, descargue el catálogo más reciente para mostrar el último informe de comparación.
- Cuando actualiza a esta versión de DLCI para SCVMM, la información más reciente no se muestra para los servidores descubiertos en versiones anteriores. Para obtener la última información del servidor y corregir el informe de comparación, vuelva a descubrir los servidores.

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

1. En **Complemento de consola de DLCI para SCVMM**, en **Centro de mantenimiento**, seleccione un grupo de actualización en **Seleccionar grupo de actualización**.
2. (Opcional) Para cambiar el origen de actualizaciones, seleccione un origen de actualizaciones desde **Seleccionar origen de actualizaciones**.
3. Para ver información de firmware de la versión actual, la versión de línea base y la acción de actualización recomendada por el servidor, expanda el grupo de servidores desde **Device Group/Servers (Grupo de dispositivos/servidores)** a nivel de servidor y, a continuación, a nivel de componentes.

NOTA:

Cuando visualiza la información de nivel de componentes, la información relacionada con la tarjeta de interfaz de red (NIC) de la 11.^a generación de servidores PowerEdge aparece como se indica a continuación:

- Después de aplicar filtros basados en el **tipo de actualización** cuando este es **urgente**, aparece un informe con los componentes que solo tienen actualizaciones urgentes. Si se exporta este informe, entonces también se exportan los componentes con acciones de degradación que, a su vez, tienen una actualización crítica.
- Cuando hay varias interfaces de red disponibles en una sola tarjeta NIC, solo existe una anotación para todas las interfaces en la lista **Información del componente**. Una vez aplicada la actualización del firmware, se actualizan todas las tarjetas NIC.

- Cuando se agrega una tarjeta NIC junto con las tarjetas existentes, la tarjeta NIC agregada recientemente se detalla como otra instancia en la lista **Información del componente**. Una vez aplicada la actualización del firmware, se actualizan todas las tarjetas NIC.

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

Exportación de perfiles de servidor

Puede exportar 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 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 para un servidor o grupo de servidores inmediatamente o programar la exportación para una fecha posterior. Además, puede seleccionar la opción de repetición pertinente para la frecuencia con la cual se exportan los perfiles de 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.

i NOTA:

- Asegúrese de que el trabajo **Automatic Backup (Copia de seguridad automática)** en iDRAC no se haya programado en el mismo tiempo.
- No puede exportar perfiles de servidor después de aplicar los filtros. Para exportar perfiles de servidor, borre todos los filtros aplicados.

Creación de trabajos de exportación

Para exportar las configuraciones de servidor:

Requisitos previos: deshabilite la opción **F1/F2 Prompt on Error (Indicador de F1/F2 en caso de error)** en **BIOS Settings (Configuración del BIOS)**.

1. En **Complemento de consola de DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Exportar perfil de servidor**.
2. En **Exportar perfil**, proporcione los detalles del trabajo y, a continuación, seleccione un almacén de protección. En **Exportar perfil del servidor** seleccione:
 - **Ejecutar ahora:** seleccione esta opción para exportar la configuración del servidor inmediatamente de los servidores o grupos de servidores seleccionados.
 - **Schedule (Programa):** proporcione un programa para exportar la configuración del 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.

Cancelación de trabajos de exportación de configuración de servidor

Para cancelar un trabajo de exportación:

1. En **Complemento de consola de DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Administrar trabajos**.
2. Seleccione **Exportar e importar trabajos** desde el filtro, seleccione los trabajos que desea cancelar y asegúrese de que el trabajo está en estado **Programado**.
3. Haga clic en **Cancelar** y, a continuación, haga clic en **Sí**.

Importación del perfil del 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 del servidor al estado almacenado en el perfil. En tales casos, puede

reemplazar el perfil de servidor en dicho servidor o grupo de servidores mediante la importación de un perfil exportado anteriormente de ese servidor o grupo de servidores.

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 la 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 de ese servidor o grupo de servidores en particular, el trabajo de importación de perfil de servidor fallará en aquellos servidores que tengan perfil del servidor y un mensaje de registro se agregará a los registros de actividades con los detalles del error.
- 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 DLCI para SCVMM. 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.

Importación del perfil del servidor

Para importar el inventario de servidores detectados:

1. En **DLCI para SCVMM**, en **Centro de mantenimiento**, seleccione los servidores cuyos perfiles desea importar y haga clic en **Importar perfil de servidor**.
2. Proporcione los detalles necesarios, seleccione el **Tipo de importación del perfil de servidor** que desee y, a continuación, haga clic en **Terminar**.



NOTA: Deje en blanco la opción **Preserve Data (Conservar datos)** si no desea conservar las configuraciones de RAID presentes del servidor.

Administrar los trabajos

Todos los trabajos de actualización del firmware y de exportación e importación de la configuración del servidor se muestran con su información de estado. Además, puede cancelar solo los trabajos programados.

Cancelación de trabajos de actualización de firmware

Requisitos previos: asegúrese de que el trabajo está en estado **Scheduled (Programado)**.

Para cancelar un trabajo de actualización de firmware programado:

1. En **DLCI para SCVMM**, haga clic en **Centro de mantenimiento** y, a continuación, haga clic en **Administrar tareas**.
2. Seleccione los trabajos que desea cancelar, haga clic en **Cancelar** y, a continuación, haga clic en **Sí**.

Perfiles y plantillas

Temas:

- Acerca del perfil de credenciales
- Creación de perfil de hardware
- Modificación de un perfil de configuración de hardware
- Eliminación de perfil de hardware
- Creación de perfil de hipervisor
- Modificación de un perfil de hipervisor
- Eliminación de perfil de hipervisor
- Actualización de WinPE
- Acerca de la implementación del hipervisor
- Creación de plantilla de implementación
- Modificación de una plantilla de implementación
- Eliminación de una plantilla de implementación

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. Un perfil de credencial autentica las capacidades basadas en funciones de un usuario. El dispositivo utiliza perfiles de credenciales para conectarse con el iDRAC de los sistemas administrados.

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

Puede crear cuatro tipos de perfiles de credenciales:

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

Perfiles de credenciales predefinidos

La cuenta **FTP de sistema predeterminado** es un perfil de credenciales predefinido del tipo de credenciales de FTP que tiene el **Nombre de usuario** y la **Contraseña** como **anónimo**. No se puede editar. Este perfil se utiliza para acceder a `ftp.dell.com`.

Creación de perfil de credenciales

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

- Cuando se crea un perfil de credenciales del tipo de dispositivo, se crea una **Cuenta de ejecución** asociada en **SCVMM** para administrar el servidor y el nombre de la cuenta de ejecución es `Dell_CredentialProfileName`.
 - (Recomendado) No edite ni elimine la **Cuenta de ejecución**.
- Cuando no se crean perfiles de credenciales y no hay ningún perfil de credenciales predeterminado para iDRAC disponible, se utilizará el ajuste del perfil de credenciales de iDRAC predeterminado durante el descubrimiento automático. Se utilizará el nombre de usuario **root** y la contraseña **Calvin** predeterminados.

Para crear un perfil de credenciales:

1. En Complemento de consola de DLCI para SCVMM, realice alguna de las acciones siguientes:
 - En el escritorio, haga clic en **Crear perfil de credenciales**.
 - En el panel de navegación, haga clic en **Perfiles y plantillas > Perfil de credenciales**, y, a continuación, haga clic en **Crear**.
2. En **Perfil de credenciales**, seleccione el tipo de perfil de credenciales que desee utilizar, proporcione los detalles de credenciales de usuario y, a continuación, haga clic en **Terminar**.

NOTA: Al crear el **Perfil de credenciales del dispositivo**, seleccione **iDRAC** para que sea el perfil predeterminado del iDRAC o **CMC** para que sea el perfil predeterminado para Chassis Management Controller (CMC). Seleccione **Ninguno** si elige no establecer este perfil como un perfil predeterminado.

Modificación de perfil de credenciales

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

- Una vez creado, no puede modificar el tipo del perfil de credenciales. Sin embargo, puede modificar otros campos. Actualice la pantalla para ver las modificaciones.
- No se puede modificar un perfil de credenciales de tipo dispositivo que se utiliza para la implementación del hipervisor.

Para modificar el perfil de una credencial:

Seleccione el perfil de la credencial que desea modificar, haga clic en **Editar** y actualice el perfil según sea necesario.

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 credenciales correspondiente no está disponible en el dispositivo.
- Para eliminar el perfil de credenciales que se usa en detección de servidores, elimine la información del servidor detectado y, a continuación, elimine el perfil de credenciales.
- Para eliminar un perfil de credenciales de tipo de dispositivo que se utilice para la implementación, primero elimine los servidores implementados en el entorno SCVMM y, a continuación, elimine el perfil de credenciales.
- No puede eliminar un perfil de credenciales que se utilice en un origen de actualizaciones.

Para eliminar el perfil de una credencial:

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

Creación de perfil de hardware

Puede crear un perfil de hardware mediante el servidor con la configuración dorada y, a continuación, utilizar dicho perfil para aplicar configuraciones de hardware en los sistemas administrados.

Antes de aplicar configuraciones de hardware en los sistemas administrados, confirme que los sistemas administrados son idénticos en el servidor con la configuración de oro en los siguientes parámetros:

- Componentes disponibles
- Modelo del servidor

- Controladora RAID
- Discos:
 - Número de discos
 - Tamaño de discos
 - Tipo de discos

NOTA: Una vez que haya actualizado la versión 1.0.1 de DLCI para SCVMM a la versión 1.2, edite y guarde los perfiles de hardware creados en la versión 1.2 de DLCI para SCVMM antes de aplicarlos en los servidores.

Para crear un perfil de hardware:

1. En la página DLCI Console Add-in for SCVMM (Complemento de consola de DLCI para SCVMM), realice alguna de las acciones siguientes:
 - En el escritorio, haga clic en **Crear perfil de hardware**.
 - En el panel de navegación, haga clic en **Propiedades y plantillas > Perfil de hardware**, a continuación, haga clic en **Crear**.
2. En la pantalla de bienvenida del **Perfil de hardware**, haga clic en **Siguiente**.
3. En **Perfil**, proporcione el nombre y la descripción del perfil y la IP del iDRAC del servidor de referencia y, a continuación, haga clic en **Siguiente**.

Los detalles del hardware del servidor de referencia se recolectan y se guardan como el perfil necesario. Durante la implementación, se aplica este perfil a los servidores.

4. En **Detalles del perfil**, seleccione los ajustes de BIOS, inicio y RAID y personalice DHS en función de los requisitos y, a continuación, haga clic en **Siguiente**.

NOTA:

Independientemente de sus preferencias de selección, toda la información se recopila durante la creación de perfiles de hardware; sin embargo, durante la implementación, solo se aplican sus preferencias.

Por ejemplo, si ha seleccionado una configuración de RAID, se recopila toda la información de configuración de RAID, inicio y BIOS; sin embargo, solo los ajustes de RAID se aplican durante la implementación.

No se admite la configuración del controlador SATA de conjunto de chips que aparece en la **Configuración de RAID**.

5. En **Resumen**, haga clic en **Terminar**.

Puede utilizar este perfil de hardware y aplicarlo a los sistemas administrados requeridos.

Modificación de un perfil de configuración de hardware

Tenga en cuenta lo siguiente al modificar un perfil de configuración de hardware:

- Puede modificar la configuración del BIOS y la secuencia de arranque.
- Para los servidores PowerEdge de 11.^a y 12.^a generación, puede modificar DHS para RAID como **One (Uno)** o **None (Ninguno)** y para los servidores PowerEdge de 13.^a generación, solo puede conservar la configuración RAID existente del servidor.

Para modificar un perfil de configuración de hardware:

1. En el complemento de consola de DLCI para SCVMM, haga clic en **Perfil de hardware**.
2. Seleccione el perfil que desea modificar y haga clic en **Editar**.

NOTA: No se admite la configuración del controlador SATA de conjunto de chips que aparece en la Configuración de RAID.

3. Realice los cambios necesarios y haga clic en **Terminar**.

Eliminación de perfil de hardware

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

- Si elimina un perfil de hardware, se actualiza la plantilla de implementación asociada con este perfil de hardware.

Para eliminar un perfil de configuración de hardware:

1. En el complemento de consola de DLCI para SCVMM, haga clic en **Perfil de hardware**.

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

Creación de perfil de hipervisor

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

Requisitos previos:

- Se crea la ISO de WinPE necesaria y la ISO está disponible en la carpeta de recurso compartido de la Gateway de integración de DLCI para SCVMM. Para actualizar una imagen de WinPE, consulte [Actualización de la imagen de WinPE](#).
- En SCVMM, se crea un grupo de hosts, un perfil de host o un perfil de equipo físico.

Para crear un perfil de hipervisor:

1. En Complemento de consola de DLCI para SCVMM, realice alguna de las acciones siguientes:
 - En el escritorio, haga clic en **Crear perfiles de hipervisor**.
 - En el panel de navegación de la izquierda, haga clic en **Perfiles y plantillas Perfiles de hipervisor** y, a continuación, haga clic en **Crear**.
2. En el **Asistente para perfiles de hipervisor**, en la página **Bienvenida**, haga clic en **Siguiente**.
3. En **Perfil de hipervisor**, proporcione un nombre y una descripción para el perfil y, a continuación, haga clic en **Siguiente**.
4. En la página de información de **SCVMM**, introduzca la información del **SCVMM Host Group Destination (Destino de grupo de hosts de SVMM)** y el **SCVMM Host Profile/Physical Computer Profile (Perfil de host de SCVMM o Perfil de equipo físico)**.
5. En **Fuente de la imagen de arranque de WinPE**, ingrese la información `<Network WinPE ISO file name>.iso` y haga clic en **Siguiente**.
6. (Opcional) Para activar la inyección de LC; si está activada, seleccione el sistema operativo que desea implementar de modo que se recojan los controladores adecuados. Seleccione **Habilitar LC Drivers Injection** y en **Versión de hipervisor**, seleccione la versión de hipervisor necesaria.
7. En **Resumen**, haga clic en **Terminar**.

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 podrá modificar la ISO.

Para modificar un perfil de hipervisor:

1. En el complemento de consola de DLCI para SCVMM, en **Perfil de hipervisor**, seleccione el perfil que desea modificar y haga clic en **Editar**.
2. Proporcione los detalles y haga clic en **Terminar**.

Eliminación de perfil de hipervisor

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

- Si se elimina un perfil de hipervisor, también se elimina la plantilla de implementación asociada con dicho perfil.

Para eliminar un perfil de hipervisor:

En el complemento de consola de DLCI para SCVMM, en **Perfil de hipervisor**, seleccione el perfil que desea eliminar y haga clic en **Eliminar**.

Actualización de WinPE

Se necesita un servidor de entorno previo a la ejecución (PXE) de SCVMM para crear una imagen de WinPE. La ISO de WinPE se crea a partir de la imagen de WinPE y Dell OpenManage Deployment Toolkit (DTK).

NOTA: Mientras utiliza la versión más reciente del DTK para crear una imagen ISO de WinPE, utilice el archivo **Dell OpenManage Deployment Toolkit para Windows**. El archivo **Dell 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 OpenManage Deployment Toolkit Windows Driver Cabinet** para la actualización de WinPE.

Para crear una imagen ISO de WinPE:

1. Agregar el servidor PXE en el appliance.
2. Después de agregar el servidor PXE, copie el archivo `boot.wim` desde el servidor PXE a la carpeta WIM del recurso compartido de la Gateway de integración de DLCI para SCVMM. El `boot.wim` se encuentra en la siguiente ruta:
`C:\RemoteInstall\DCMgr\Boot\Windows\Images.`

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

DTK es un archivo ejecutable autoextraíble.

Para trabajar con DTK:

1. Haga doble clic en el archivo ejecutable de DTK.
2. Seleccione la carpeta para extraer los controladores de DTK, por ejemplo `C:\DTK501`.
3. Copie la carpeta de DTK que se extrajo a la carpeta de recurso compartido de DTK de la puerta de enlace de integración. Por ejemplo, `\\DLCI IG Share\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.

Para actualizar una imagen de WinPE:

1. En la consola de DLCI, seleccione **Actualización de WinPE**, en **Origen de la imagen**, para **Ruta de acceso a imagen de WinPE personalizada**, proporcione la ruta de acceso de la imagen de WinPE.
Por ejemplo, `import.xml`.
2. En **DTK Path (Ruta de acceso de DTK)**, para **DTK Drivers Path (Ruta de acceso de controladores de DTK)**, proporcione la ubicación de los controladores de Dell Deployment Toolkit.
Por ejemplo, `import.xml`.
3. Proporcione el nombre de ISO.
4. 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).
5. Haga clic en **Actualizar**.
La ISO de WinPE con el nombre proporcionado en el paso anterior se crea en `\\DLCI IG Share\ISO`.

Acerca de la implementación del hipervisor


La implementación del hipervisor es un flujo de trabajo basado en perfiles. Este flujo de trabajo permite especificar las configuraciones del hardware, del hipervisor y del SCVMM, como también la fuente de actualización para las actualizaciones del firmware. Además, puede continuar con la implementación del hipervisor incluso si la actualización del firmware falla. Sin embargo, todos los componentes de los servidores o grupos de servidores seleccionados se actualizan durante la implementación del hipervisor. Este flujo de trabajo utiliza una red lógica y un perfil de host disponible en SCVMM necesario en el momento de la creación del perfil de hipervisor junto con la configuración del hardware para la implementación del hipervisor en el dispositivo. La implementación del hipervisor es compatible con la implementación de uno a uno y de uno a varios.

Creación de plantilla de implementación

Puede crear plantillas de implementación con los perfiles de hipervisor y de hardware necesarios, además de una fuente de actualización, y aplicar la plantilla de implementación a los servidores sin asignar. Le permite crear la plantilla una vez y utilizarla varias veces.

Para crear una plantilla de implementación:

1. En el servidor, realice cualquiera de las acciones siguientes:
 - En el tablero de control del servidor, haga clic en **Crear plantilla de implementación**.

- En el panel de navegación del servidor, haga clic en **Perfiles y plantillas** y, a continuación, haga clic en **Plantilla de implementación**.
2. En **Plantilla de implementación**, introduzca el nombre de la plantilla y una descripción para la misma y, a continuación, seleccione un perfil de hipervisor, el perfil de hardware, y el origen de actualización.
 3. (Opcional) Seleccione un origen de actualización y un perfil de hardware y, para continuar con la implementación, incluso si la actualización de firmware falla, seleccione **Continuar OSD aunque falle la actualización de firmware**.
 **NOTA:** De manera predeterminada no se admite la degradación.
 4. (Opcional) Si no se crea el perfil de hardware o hipervisor, puede crearlos haciendo clic en **Crear nuevo**.


Modificación de una plantilla de implementación

 **NOTA:** Puede modificar el nombre, la descripción y la selección del perfil de hipervisor, perfil de hardware y origen de actualizaciones.

Para modificar una plantilla de implementación:

1. En Complemento de consola de DLCI para SCVMM, haga clic en **Plantillas de implementación**.
2. Seleccione la plantilla de implementación que desea modificar y haga clic en **Editar**.
3. Realice los cambios necesarios y haga clic en **Terminar**.

Eliminación de una plantilla de implementación

 **NOTA:** La eliminación de una plantilla de implementación no afecta al hardware asociado, los perfiles de hipervisor ni el origen de actualización.

Para eliminar una plantilla de implementación:

1. En Complemento de consola de DLCI para SCVMM, haga clic en **Plantillas de implementación**.
2. Seleccione la plantilla de implementación que desea eliminar y haga clic en **Eliminar**.

Implementación de hipervisores

Los sistemas operativos se implementan solo en servidores compatibles.

Antes de la implementación de hipervisores, tenga en cuenta lo siguiente: actualice las versiones de firmware a las versiones más recientes disponibles en ftp.dell.com o downloads.dell.com y continúe con la implementación del hipervisor.

Para implementar en servidores:

1. En el servidor haga lo siguiente:
 - En el tablero de control del servidor, haga clic en **Implementar servidores sin asignar**.
 - En el panel de navegación del servidor, haga clic en **Asistente de implementación**.
2. En **Bienvenido**, haga clic en **Siguiente**.
3. En **Seleccionar servidores**, seleccione los servidores en los que desea implementar las licencias, busque si hay licencias disponibles y, a continuación, haga clic en **Siguiente**.
4. En **Seleccionar plantilla y perfil**, seleccione la plantilla de implementación adecuada y el perfil de credenciales de tipo dispositivo asociado.

NOTA:

- Asegúrese de seleccionar el perfil de hipervisor creado por usted para visualización en pantalla (OSD) y las tareas de actualización del firmware.
- Puede asignar múltiples perfiles de credenciales para varios servidores.

También puede crear una plantilla de implementación y un perfil de credenciales.

5. En **Identificación de servidores**, seleccione los servidores y proporcione el nombre de host, la dirección MAC y la información de red estática o DHCP que desea aplicar a los servidores y, a continuación, haga clic en **Siguiente**.
6. En **Detalles del trabajo**, proporcione un nombre para el trabajo a fin de realizar el seguimiento de dicho trabajo y del estado de la implementación y haga clic en **Siguiente**.
7. En **Resumen**, vea las opciones de implementación que ha proporcionado y haga clic en **Terminar**.
8. En el mensaje **Confirmación**, haga clic en **Sí**.

NOTA:

Descargue e instale los controladores que correspondan en dell.com/support si aparece un icono de advertencia amarillo en **Administrador de dispositivos** después de implementar el sistema operativo Windows 2016 en servidores Dell PowerEdge de 12.ª generación.

Visualización de información en el appliance

Temas:

- Centro de tareas y registros
- Visualización de tareas administradas
- Cancelar tareas programadas

Centro de tareas y registros

En la página **Centro de trabajos y registros** se incluye información sobre todas las actividades que se iniciaron en DLCI para SCVMM. Puede ver el estado del progreso de un trabajo y su subtarea. Además, puede filtrar y ver los trabajos para una categoría específica. Puede ver los trabajos desde el portal de administración de DLCI/SCVMM y el complemento de la consola de DLCI para SCVMM. Los usuarios o el sistema generan los nombres de los trabajos y las subtareas reciben el nombre de la dirección IP o nombre de host del servidor administrado. Expanda la subtarea para ver los registros de actividad para ese trabajo. Hay cuatro categorías de trabajos:

- Running (En ejecución): muestra todas las tareas que actualmente están en ejecución, o en estado de progreso.
- History (Historial): muestra todas las tareas que se ejecutaron anteriormente con su estado de tarea.
- Programado: muestra todos los trabajos programados para una fecha y hora posteriores. Además, puede cancelar los trabajos programados.
- Generic Logs (Registros genéricos): muestra mensajes de registro comunes y específicos del dispositivo que no son específicos de tareas secundarias y otras actividades.
 - Mensajes de registro de dispositivo: muestra todos los mensajes de registro específicos de dispositivos, como el reinicio del dispositivo. Solo puede ver esta categoría de mensajes desde el portal de administración.
 - Generic Log Messages (Mensajes de registro genérico): muestra todos los mensajes de registro que son comunes para las tareas que se muestran en las pestañas **Running (En ejecución)**, **History (Historial)** y **Scheduled (Programado)**.

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 SUU de esa tarea.

Los distintos estados de tarea del dispositivo son los siguientes:

- Canceled (Cancelada): el usuario canceló manualmente la tarea o se canceló cuando se reinició el dispositivo.
- Successful (Exitosa): la tarea se ha ejecutado satisfactoriamente.
- Failed (Error): no se pudo completar la tarea.
- In Progress (En curso): la tarea se está ejecutando.
- Scheduled (Programada): la tarea se ha programado para otra fecha.
- Waiting (En espera): la tarea está en cola para comenzar a ejecutarse.
- Recurring Schedule (Programa periódico): tarea recurrente después de un intervalo fijo de tiempo.

NOTA: Cuando se programan los mismos trabajos al mismo tiempo, por los mismos usuarios u otros, el trabajo puede fallar. Por lo tanto, asegúrese de que los mismos trabajos no se programen al mismo tiempo.

Para ver el centro de tareas y registros:

1. En **DLCI para SCVMM**, haga clic en **Centro de tareas y registros**.

De manera predeterminada, se muestra la pestaña **Running (En ejecución)**.

2. Para ver una categoría específica de tareas, haga clic en la pestaña que corresponda.

Expanda la categoría del trabajo para ver todos los servidores 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**.
- Después de actualizar a la versión 1.3 de DLCI para SCVMM, no habrá información disponible de las tareas secundarias de las tareas que se ejecutando con versiones anteriores de DLCI para SCVMM en la pestaña **History (Historial)**.

3. (Opcional) Filtre las tareas según el tipo de tarea.

Visualización de tareas administradas

Puede ver todos los trabajos enviados a 1610 desde la página **Centro de mantenimiento**.

En 1610, realice cualquiera de las siguientes acciones:

- 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**.

Todos los trabajos programados se muestran con el nombre, el tipo, la descripción, el estado y la fecha de inicio y de finalización del trabajo.

Cancelar tareas programadas

1. En Complemento de consola de DLCI para SCVMM, realice alguna de las acciones siguientes:
 - 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 las tareas que desea cancelar y haga clic en **Cancelar**.

Solución de problemas

Temas:

- El grupo de actualización de clúster vacío no se elimina durante el descubrimiento automático o la sincronización
- Trabajos de descubrimiento no enviados
- Creación de grupos de chasis VRTX duplicados
- Exportación de perfil de configuración de otro servidor tras cambiar la dirección IP
- Error al aplicar la configuración de RAID
- Error de creación de origen de actualización
- Error de actualización de firmware porque la de cola de trabajos está llena
- Error al actualizar el firmware utilizando la fuente de actualización de DRM
- Error de un trabajo programado en un grupo de actualización
- Error de actualización del firmware en grupo actualización de clúster
- Error al actualizar el firmware en 11.a generación de servidores
- Error al conectarse con FTP mediante el origen de actualizaciones predeterminado del sistema
- Error al crear un repositorio durante una actualización del firmware
- Error al eliminar un grupo de actualización personalizado
- Error al exportar registros de LC en formato CSV
- Error al ver los registros de LC
- Error al exportar perfiles de servidores
- Actualización del firmware en algunos componentes independientemente de la selección
- Problema de instalación de IG mientras se ejecutan varias instancias del instalador en el mismo servidor
- La importación del trabajo de perfil de servidor agota el tiempo de espera después de dos horas
- Error de implementación de hipervisores
- Error de implementación del hipervisor debido a archivos de controlador retenidos en el recurso compartido de biblioteca
- La información de inventario más reciente no aparece incluso después una actualización del firmware
- Error 21119 de SCVMM VMM al agregar servidores Active Directory
- La implementación del hipervisor falla en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory
- Error de configuración de RAID para discos virtuales con RAID10
- Error de configuración de RAID debido a la configuración de repuestos dinámicos en RAID de software S130

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

Cuando se descubre un grupo de clúster en el dispositivo, 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.

Trabajos de descubrimiento no enviados

Cuando presione la tecla de retroceso para descartar un mensaje de error en la pantalla de descubrimiento, los trabajos de descubrimiento posteriores no se envían para el procesamiento interno.

Como solución alternativa, cierre la pantalla de descubrimiento actual y vuelva a iniciar la pantalla de descubrimiento desde la página **Inventario**. Envíe el nuevo trabajo de descubrimiento después de ingresar las entradas necesarias.

Creación de grupos de chasis VRTX duplicados

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

Para solucionar este problema, realice lo siguiente:

1. Extraiga un servidor modular de un chasis y agréguelo en otro chasis. Para obtener más información, consulte la sección Módulos del servidor en *Manual del propietario del gabinete Dell PowerEdge VRTX*.
2. Configuración de la CMC. Para obtener más información, consulte Instalación y ajuste de la CMC en la *Guía del usuario de Chassis Management Controller versión 2.1 para Dell PowerEdge VRTX* disponible en dell.com/support/home.

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

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

Exportación de perfil de configuración de otro servidor tras cambiar la dirección IP

Después de haber programado un trabajo **Export Server Profile (Exportar perfil del servidor)** en un servidor, si la dirección IP de este servidor se asigna a otro servidor, entonces el servidor exportará el perfil de servidor de este nuevo servidor.

Para solucionar este problema, cancele el trabajo **Export Server Profile (Exportar perfil de servidor)**, vuelva a detectar el servidor cuya dirección IP ha cambiado y, a continuación, programe el trabajo **Export Server Profile (Exportar perfil de servidor)** en este servidor.

Error al aplicar la configuración de RAID

La aplicación de un perfil de hardware con configuración de RAID puede fallar con los siguientes mensajes de error: `Error An unknown exception has occurred and has been logged in the extended logs.`

```
Error RAID configuration failed with error: An unknown exception has occurred and has been logged in the extended logs. <iDRAC IP address>
```

```
Error 0_EX_MSG
```

Para solucionar este problema, realice un **Ciclo de encendido del sistema** del servidor y vuelva a aplicar la configuración de hardware.

Error de creación de origen de actualización

Cuando se cambia la configuración de red del sistema de nombres de dominio (DNS) del servidor, la creación del tipo HTTP o FTP de origen de actualización falla.

Para solucionar este problema, reinicie el servidor y, a continuación, cree el origen de actualización de tipo HTTP o FTP.

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

Los trabajos de actualización del firmware enviado desde el dispositivo a iDRAC fallan y en el registro principal del dispositivo 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.

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

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

Para solucionar este problema, realice lo siguiente:

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

Error de un trabajo programado en un grupo de actualización

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

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

Error de actualización del firmware en grupo actualización de clúster

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

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

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

Un trabajo de actualización de firmware que comenzó en los servidores Dell PowerEdge de 11.ª generación puede fallar debido a versiones incompatibles de iDRAC y LC, y se muestra el siguiente error: `WSMAN command failed to execute on server with iDRAC IP <IP address>`.

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

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

Después de instalar y configurar, o de actualizar el servidor, el intento de acceder al sitio FTP con un **catálogo en línea de Dell** de origen de actualización creado por el sistema podría fallar si se necesitan credenciales de proxy.

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

Error al crear un repositorio durante una actualización del firmware

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

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

Error al eliminar un grupo de actualización personalizado

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

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

Error al exportar registros de LC en formato CSV

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

Como solución alternativa, agregue el dispositivo FQDN en el navegador en el sitio de intranet local. Para obtener información sobre cómo agregar el dispositivo en la intranet local, consulte la sección [Visualización de registros de LC](#).

Error al ver los registros de LC

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

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

Error al exportar perfiles de servidores

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

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

Actualización del firmware en algunos 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 servidores individuales. Este comportamiento se observa en los servidores Dell PowerEdge de 12.^a y 13.^a generaciones con licencia de iDRAC Enterprise.

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

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

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

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

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

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

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

Para solucionar este problema, realice los pasos siguientes:

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

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

Error de implementación de hipervisores

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

Este error puede ocurrir debido a alguna de estas razones:

- El estado de Dell Lifecycle Controller es defectuoso.

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

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

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

Consulte el siguiente artículo de KB para solucionar este problema: support.microsoft.com/KB/961804.

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

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

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

Estos 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**, luego seleccione el servidor de la puerta de enlace de integración 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 Gateway de integración mediante `\\<Integration Gateway server>\LCDriver\.`
4. Elimine la carpeta que contiene los archivos del controlador.

Ahora puede implementar sistemas operativos.

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

Aunque el trabajo de actualización de firmware se ha completado en un servidor Dell PowerEdge de 11.ª generación, en el appliance, el inventario no muestra las versiones de firmware más recientes.

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

Como solución alternativa, verifique si se terminó la actividad de CSIOR en el servidor PowerEdge y, a continuación, actualice el inventario del firmware en el dispositivo. Además, asegúrese de reiniciar el servidor después de aplicar la actualización preconfigurada sin agente. Para obtener más información sobre la actualización del inventario, consulte [Visualización y actualización del inventario del firmware](#).

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

Error 2119 de SCVMM VMM al agregar servidores Active Directory

Cuando se agregan servidores a Active Directory, aparece el error 2119 de SCVMM. `Error 2119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

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. Una vez agregado el servidor a SCVMM, vuelva a detectarlo en la consola de DLCI.
El servidor aparece en la pestaña **Host**.

La implementación del hipervisor falla en los servidores blade PowerEdge de 11.ª generación cuando se utiliza Active Directory

La implementación del hipervisor falla en los servidores blade PowerEdge de 11.ª generación cuando se utiliza la información de identificación de Active Directory. Los servidores blade PowerEdge de 11.ª generación usan el protocolo de interfaz de administración de plataforma inteligente (IPMI, por sus siglas en inglés) para la comunicación. Sin embargo, la IPMI no es compatible con el uso de credenciales de la configuración de Active Directory.

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

Error de configuración de RAID para discos virtuales con RAID10

La configuración de RAID falla cuando se crean discos virtuales con nivel RAID 10 para la controladora H200 mediante el uso de más de cuatro discos físicos.

Error de RAID 10 con más de cuatro discos físicos.

Como solución, utilice el número mínimo de discos físicos necesarios para ese nivel RAID.

Error de configuración de RAID debido a la configuración de repuestos dinámicos en RAID de software S130

La configuración de RAID en la controladora RAID de software S130 falla cuando se intenta configurar RAID con más de tres repuestos dinámicos, incluido el repuesto dinámico global (GHS) y DHS.

Para solucionar este problema:

- Utilice solo tres repuestos dinámicos (GHS y DHS) para aplicar en un perfil.
- Utilice la tarjeta de controladora RAID PowerEdge (PERC).

Acceso a contenido de soporte desde el sitio de soporte de Dell EMC

Acceda al contenido de soporte relacionado con un arreglo de herramientas de administración de sistemas mediante enlaces directos, vaya al sitio de soporte de Dell EMC o use un motor de búsqueda.

- Enlaces directos:
 - Para Dell EMC Enterprise Systems Management y Dell EMC Remote Enterprise Systems Management:<https://www.dell.com/esmmanuals>
 - Para Dell EMC Virtualization Solutions:<https://www.dell.com/SoftwareManuals>
 - Para Dell EMC OpenManage:<https://www.dell.com/openmanagemanuals>
 - Para iDRAC:<https://www.dell.com/idracmanuals>
 - Para Dell EMC OpenManage Connections Enterprise Systems Management:<https://www.dell.com/OMConnectionsEnterpriseSystemsManagement>
 - Para Dell EMC Serviceability Tools:<https://www.dell.com/serviceabilitytools>
- Sitio de soporte 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 enlace necesario.
 4. Haga clic en el producto necesario y, luego, haga clic en la versión necesaria.

Mediante los motores de búsqueda, escriba el nombre y la versión del documento en el cuadro Buscar.