Guía del usuario de Dell EMC OpenManage Enterprise, versión 3.6

Junio 2021
Rev. A00

Notas, precauciones y advertencias

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

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

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

Tabla de contenido

Tablas

1

Acerca de Dell EMC OpenManage Enterprise

OpenManage Enterprise es una aplicación web de administración y monitoreo de sistemas que se entrega como un dispositivo virtual. Proporciona una vista completa de los servidores Dell EMC, el chasis, el almacenamiento y los switches de red en la red empresarial. Con OpenManage Enterprise, una aplicación basada en la Web de administración general de sistemas, los usuarios pueden hacer lo siguiente:

- Detectar dispositivos en un entorno de centro de datos.
- Ver el inventario de hardware y monitorear el estado de los dispositivos.
- Ver y administrar las alertas que recibió el dispositivo y configurar políticas de alerta.
- Monitorear las versiones de firmware/controlador y administrar las actualizaciones de firmware/controlador en los dispositivos con bases de firmware.
- Administrar tareas remotas (como control de alimentación) en los dispositivos.
- Administrar los ajustes de configuración en los dispositivos mediante plantillas de implementación.
- Administrar la configuración de identidad virtual en los dispositivos mediante grupos inteligentes de identidad.
- Detectar y corregir las desviaciones de configuración en los dispositivos mediante bases de configuración.
- Recuperar y monitorear la información de garantía para los dispositivos.
- Agrupar dispositivos en grupos estáticos o dinámicos.
- Crear y administrar usuarios de OpenManage.

NOTA:

- La administración y el monitoreo de sistemas de OpenManage Enterprise son más adecuados para las redes LAN empresariales y no se recomienda su uso mediante redes WAN.
- Para obtener más información sobre los navegadores compatibles, consulte la *Matriz de soporte de OpenManage Enterprise* disponible en el sitio de soporte técnico.

Algunas de las características de seguridad de OpenManage Enterprise son las siguientes:

- Acceso basado en funciones que limita el acceso a las configuraciones de la consola y a las acciones del dispositivo.
- El control de acceso basado en el alcance permite a los administradores restringir los grupos de dispositivos a los que pueden acceder y en los que pueden gestionar los administradores de dispositivos.
- Servidor reforzado con Security-Enhanced Linux (SELinux) y un firewall interno.
- Cifrado de datos confidenciales en una base de datos interna.
- Uso de comunicación cifrada fuera del servidor (HTTP).
- Crear y aplicar políticas relacionadas con firmware y configuración.
- Provisión para configurar y actualizar los servidores de metal descubierto.

OpenManage Enterprise posee una GUI basada en tareas de dominio, en la que la navegación está diseñada pensando en la secuencia de tareas que utilizan principalmente los administradores y administradores de dispositivos. Cuando agrega un dispositivo a un entorno, OpenManage Enterprise detecta automáticamente las propiedades del dispositivo, lo pone en el grupo de dispositivos pertinente y le permite administrar el dispositivo. La secuencia normal de tareas que realizan los usuarios de OpenManage Enterprise:

- Instalar OpenManage Enterprise en la página 20
- Configurar OpenManage Enterprise con interfaz de usuario de texto en la página 27
- Detección de dispositivos para la supervisión o administración en la página 40
- Administrar dispositivos y grupos de dispositivos en la página 54
- Monitoreo de dispositivos mediante el panel de OpenManage Enterprise en la página 37
- Organizar los dispositivos en grupos en la página 54
- Administrar el firmware y los controladores del dispositivo en la página 75
- Ver y configurar dispositivos individuales en la página 67
- Monitoreo y administración de alertas de dispositivos en la página 117
- Ver y renovar la garantía del dispositivo en la página 137
- Administrar plantillas de implementación de dispositivos en la página 85
- Administración del cumplimiento de la configuración del dispositivo en la página 109
- Administrar plantillas de cumplimiento en la página 110
- Monitoreo de registros de auditoría en la página 126
- Administración de los ajustes del servidor OpenManage Enterprise en la página 146

- Ejecución de un trabajo de inventario ahora en la página 73
- Administración de la garantía del dispositivo en la página 136
- Informes en la página 138
- Administración de archivos de MIB en la página 143
- Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Integración de servicios de directorio en OpenManage Enterprise en la página 155

Temas:

Novedades de esta versión

- El control de acceso basado en el alcance (SBAC) ahora permite una administración más eficiente y segura de los dispositivos detectados. Los administradores pueden determinar los grupos de dispositivos que se espera que administren los administradores de dispositivos.
- Actualización de firmware sin inconvenientes en los chasis de administración de varios chasis (MCM) con soporte para un máximo de 20 chasis y sus sleds.
- Capacidad para escanear y ampliar el tamaño del disco del dispositivo en la página Interfaz de usuario de texto (TUI).
- La gama de productos soportada se expandió a los siguientes servidores Intel® Xeon® de 3.ª generación con tecnología de PowerEdge YX5X (15G): R650, R750, R750xa, MX750c, C6520.

Mejoras

- El protocolo Redfish es soportado para la detección, el inventario y el monitoreo, así como para la administración limitada (control de energía, parpadeo, diagnóstico e informes de soporte técnico) en los dispositivos con iDRAC9 4.40.10.10 y versiones posteriores.
- Se agregó un nuevo widget de utilización de recursos a la página de inicio para mostrar gráficamente la utilización de CPU y memoria por parte del dispositivo.
- Un gráfico de anillos adicional en la página Todos los dispositivos para mostrar datos del plug-in instalado.
- Se agregó la funcionalidad de correo electrónico de prueba a la configuración de SMTP.
- Se agregó la compatibilidad con SNMPv3 para el reenvío de alertas.
- Se agregó el filtrado de garantías a Ajustes de garantía para personalizar la página de garantía y los informes.

Otra información útil

Además de esta guía, puede acceder a los siguientes documentos en los que se proporciona más información sobre OpenManage Enterprise y otros productos relacionados.

Tabla 1. Otra información útil

Documento	Descripción	Disponibilidad
Matriz de compatibilidad de Dell EMC OpenManage Enterprise	Permite ver los dispositivos compatibles con OpenManage Enterprise.	1. Vaya a Dell.com/OpenManageManuals. 2. Haga clic en **OpenManage Enterprise** y seleccione la versión requerida de OpenManage Enterprise. 3. Haga clic en **Documentación** para tener acceso a estos documentos.
Notas de la versión Dell EMC OpenManage Enterprise	Permite obtener información sobre problemas conocidos y soluciones alternativas en OpenManage Enterprise.	
Guía del usuario de Dell EMC OpenManage Mobile	Proporciona información acerca de la instalación y el uso de la aplicación OpenManage Mobile.	
Guía del usuario de administrador de repositorios de Dell EMC	Proporciona información sobre el uso de Repository Manager para administrar las actualizaciones del sistema	
Guía de API RESTful de OpenManage Enterprise y	Permite obtener información sobre la integración de OpenManage Enterprise mediante las API de	

Tabla 1. Otra información útil (continuación)

Documento	Descripción	Disponibilidad
OpenManage Enterprise - Edición Modular	la transferencia representativa de estado (REST) y también incluye ejemplos referidos al uso de las API de REST para realizar tareas comunes.	
Guía del usuario de Dell EMC SupportAssist Enterprise	Proporciona información sobre instalación, configuración, uso y solución de problemas de SupportAssist Enterprise.	Dell.com/ServiceabilityTools

Cómo ponerse en contacto con Dell EMC

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

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

1. Vaya a Dell.com/support.
2. Seleccione la categoría de soporte.
3. Seleccione su país o región en la lista desplegable **Elegir un país o una región** ubicada al final de la página.
4. Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

Licencia de OpenManage Enterprise Advanced

NOTA: La instalación y el uso de OpenManage Enterprise no necesitan la licencia avanzada de *OpenManage Enterprise Advanced*. Solo la función de administración de configuración del servidor, que implementa configuraciones de dispositivos y verifica el cumplimiento de configuración en los servidores, requiere que la licencia de *OpenManage Enterprise Advanced* esté instalada en los servidores de destino. Esta licencia no es necesaria para crear plantillas de implementación desde un servidor.

La licencia de *OpenManage Enterprise Advanced* es perpetua y válida durante toda la vida útil del servidor; además, puede vincularse con la etiqueta de servicio de solo un servidor a la vez. OpenManage Enterprise ofrece un informe integrado para ver la lista de dispositivos y sus licencias. Seleccione **OpenManage Enterprise** > **Supervisión** > **Informes** > **Informe de licencia** y, luego, haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

NOTA: Para activar la función de administración de la configuración del servidor en OpenManage Enterprise no se requiere ninguna licencia aparte. Si la licencia de *OpenManage Enterprise Advanced* está instalada en un servidor de destino, puede usar la función de administración de configuración del servidor en dicho servidor.

Licencia OpenManage Enterprise Advanced, servidores compatibles

Puede implementar la licencia de *OpenManage Enterprise Advanced* en los siguientes servidores PowerEdge:

- Servidores YX3X que tienen las versiones de firmware 2.50.50.50 de iDRAC8 o posteriores. Las versiones de firmware de YX3X son compatibles con versiones anteriores y se pueden instalar en un hardware de YX2X. Consulte Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184.
- Servidores YX4X que tienen las versiones de firmware 3.10.10.10 de iDRAC9 o posteriores. Consulte Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184

Adquirir la licencia de OpenManage Enterprise Advanced

Puede adquirir la licencia de *OpenManage Enterprise Advanced* cuando adquiere un servidor, o bien comunicándose con su representante de ventas. Puede descargarse la licencia adquirida desde el portal de administración de licencias de software en Dell.com/support/retail/lkm.

Verificación de la información de la licencia

OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos que supervisa OpenManage Enterprise y sus licencias. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Informes** > **Informe de la licencia**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

Puede verificar si la licencia de *OpenManage Enterprise Advanced* está instalada en un servidor mediante:

- En todas las páginas de OpenManage Enterprise, en la esquina superior derecha, haga clic en el símbolo **i** y, a continuación, haga clic en **Licencias**.
- En el cuadro de diálogo **Licencias**, lea el mensaje y haga clic en los enlaces correspondientes para ver y descargar archivos de código fuente abierto relacionados con OpenManage Enterprise u otras licencias con código fuente abierto.

Funciones basadas en la licencia en OpenManage Enterprise

Se requiere la licencia de *OpenManage Enterprise Advanced* para usar las siguientes funciones de OpenManage Enterprise:

- Implementación de la configuración del servidor.
- Creación y corrección de la línea base de cumplimiento de normas del servidor.
- Iniciar desde ISO.
- Active los complementos disponibles, como Power Manager, para ampliar la capacidad del dispositivo.

NOTA: Para acceder a las funciones de OpenManage Enterprise, por ejemplo, la función de soporte de la consola virtual, que depende del iDRAC, deberá tener la licencia Enterprise de iDRAC. Para obtener más información, consulte la *Documentación del iDRAC* que se encuentra en el sitio de soporte.

2

Características de seguridad en OpenManage Enterprise

Algunas de las características de seguridad de OpenManage Enterprise son las siguientes:

- El control de acceso basado en funciones permite una funcionalidad de administración de dispositivos diferente para las distintas funciones de usuario (Administrador, Administrador de dispositivos y Lector).
- El control de acceso basado en el alcance permite que un administrador determine los grupos de dispositivos que se espera que administren los administradores de dispositivos.
- Servidor reforzado con Security-Enhanced Linux (SELinux) y un firewall interno.
- Cifrado de datos confidenciales en una base de datos interna.
- Uso de comunicación cifrada fuera del dispositivo (HTTPS).
- Solo se admiten navegadores con cifrado de 256 bits. Para obtener más información, consulte Requisitos mínimos del sistema para implementar OpenManage Enterprise en la página 21

AVISO: Los usuarios no autorizados pueden obtener acceso a nivel de SO para el dispositivo OpenManage Enterprise mediante la omisión de las restricciones de seguridad de Dell EMC. Una forma es conectar el VMDK en otra VM de Linux como una unidad secundaria y obtener así acceso a la partición del sistema operativo, en la que las credenciales de inicio de sesión a nivel de sistema operativo podrían alterarse. Dell EMC recomienda a los clientes cifrar la unidad (archivo de imagen) para dificultar el acceso no autorizado. Los clientes también deben asegurarse de que con cualquier mecanismo de cifrado que se utilice, puedan posteriormente descifrar los archivos. De lo contrario, el dispositivo no podrá iniciarse.

NOTA:

- Cualquier cambio en la función del usuario se aplicará de inmediato y se cerrará la sesión activa de los usuarios afectados.
- Los usuarios del directorio AD y LDAP pueden importarse y se les puede asignar uno de los roles de OpenManage Enterprise (administrador, administrador de dispositivos o visor).
- Para ejecutar las acciones de administración de dispositivos, se requiere una cuenta con privilegios apropiados de usuario en el dispositivo.

Información relacionada

Instalar OpenManage Enterprise en la página 20

Temas:

Tipos de roles de usuario en OpenManage Enterprise

NOTA:

- Los usuarios del directorio AD y LDAP pueden importarse y se les puede asignar uno de los roles de OpenManage Enterprise (administrador, administrador de dispositivos o visor).
- Las acciones que se ejecutan en los dispositivos requieren una cuenta con privilegios en el dispositivo.

Tabla 2. Tipos de roles de usuario en OpenManage Enterprise

El usuario con este rol...	Tiene los siguientes privilegios del usuario
Administrador	Tiene acceso completo a todas las tareas que se pueden realizar en la consola.

Tabla 2. Tipos de roles de usuario en OpenManage Enterprise (continuación)

El usuario con este rol...	Tiene los siguientes privilegios del usuario
	• Acceso total (mediante GUI y REST) para leer, ver, crear, editar, eliminar, exportar y quitar información relacionada con los dispositivos y grupos que supervisa OpenManage Enterprise. • Puede crear usuarios de Microsoft Active Directory (AD), de LDAP y locales, y asignar roles adecuados • Activar y desactivar usuarios • Modificar los roles de los usuarios existentes • Eliminar los usuarios • Cambiar la contraseña de usuario
Administrador de dispositivos (DM)	• Ejecutar tareas, políticas y otras acciones en los dispositivos (alcance) asignados por el administrador.
Observador	• Solo puede ver la información que se muestra en OpenManage Enterprise y ejecutar informes. • De manera predeterminada, tiene acceso de solo lectura a la consola y todos los grupos. • No se puede ejecutar las tareas ni crear y administrar políticas.

NOTA:

- Si un observador o DM se cambia a administrador, se consiguen privilegios completos de administrador. Si un observador se cambia a un DM, el observador tiene los mismos privilegios de un DM.
- Cualquier cambio en la función del usuario se aplicará de inmediato y se cerrará la sesión activa de los usuarios afectados.
- El registro de auditoría se realiza en los siguientes casos:
  - Se asignan o cambian los permisos de acceso de un grupo.
  - Se modifica el rol de usuario.

Tareas relacionadas

Instalar OpenManage Enterprise en la página 20

Información relacionada

Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Control de acceso basado en funciones y en el alcance en OpenManage Enterprise

OpenManage Enterprise tiene control de acceso basado en funciones (RBAC), que define claramente los privilegios de usuario para las tres funciones incorporadas: Administrador, Administrador de dispositivos y Lector. Además, mediante el control de acceso basado en el alcance (SBAC), el administrador puede limitar los grupos de dispositivos a los que el administrador de dispositivos tiene acceso. En los siguientes temas, se explican en detalle las funciones RBAC y SBAC.

Privilegios del control de acceso basado en funciones (RBAC) en OpenManage Enterprise

A los usuarios se les asignan funciones que determinan su nivel de acceso a la configuración del dispositivo y a las funciones de administración de dispositivos. Esta función se conoce como Control de acceso basado en funciones (RBAC). La consola exige el privilegio necesario para una determinada acción antes de permitirla. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte Administración de usuarios de OpenManage Enterprise en la página 147.

En esta tabla, se indican los diversos privilegios activados para cada función.

Tabla 3. Privilegios de usuario basados en roles en OpenManage Enterprise

Funciones de OpenManage Enterprise	Descripción del privilegio	Niveles de usuario para acceder a OpenManage Enterprise		
		Admin (Administrador)	Administrador de dispositivos	Observador
Configuración del dispositivo	Ajustes globales del dispositivo que implican la configuración del dispositivo.	**S**	N	N
Configuración de seguridad	Ajustes de seguridad del dispositivo	**S**	N	N
Administración de alertas	Acciones/administración de alertas	**S**	N	N
Administración de fabric	Acciones/administración de fabric	**S**	N	N
Administración de red	Acciones/administración de red	**S**	N	N
Administración de grupos	Crear, leer, actualizar y eliminar (CRUD) para grupos estáticos y dinámicos	**S**	N	N
Administración de detección	CRUD para tareas de detección, ejecución de tareas de detección	**S**	N	N
Administración de inventario	CRUD para tareas de inventario, ejecución de tareas de inventario	**S**	N	N
Administración de capturas	Importación de MIB, edición de capturas	**S**	N	N
Administración de implementación automática	Administración de operaciones de configuración de implementación automática	**S**	N	N
Configuración de monitoreo	Políticas de alerta, reenvío, SupportAssist etc.	**S**	**S**	N
Control de alimentación	Reinicio o ciclo de energía del dispositivo	**S**	**S**	N
Configuración del dispositivo	Configuración del dispositivo, aplicación de plantillas, administración/migración de identidad de IO, asignación de almacenamiento (para dispositivos de almacenamiento), etc.	**S**	**S**	N
Implementación del sistema operativo	Implementación del sistema operativo, asignación a LUN, etc.	**S**	**S**	N
Actualización del dispositivo	Actualización del firmware del dispositivo, aplicación de bases actualizadas, etc.	**S**	**S**	N
Administración de plantillas	Creación o administración de plantillas	**S**	**S**	N
Administración de base	Creación o administración de políticas de firmware o configuración de base	**S**	**S**	N
Administración de energía	Establecimiento de asignaciones de energía	**S**	**S**	N

Tabla 3. Privilegios de usuario basados en roles en OpenManage Enterprise (continuación)

Funciones de OpenManage Enterprise	Descripción del privilegio	Niveles de usuario para acceder a OpenManage Enterprise		
		Admin (Administrador)	Administrador de dispositivos	Observador
Administración de trabajos	Administración/ejecución de trabajos	**S**	**S**	N
Administración de informes	Operaciones CRUD en informes	**S**	**S**	N
Ejecución de informes	Ejecutar informes	**S**	**S**	**S**
Ver	Visualización de todos los datos, administración o ejecución de informes, etc.	**S**	**S**	**S**

Control de acceso basado en el alcance (SBAC) en OpenManage Enterprise

Con el uso de la función de control de acceso basado en funciones (RBAC), los administradores pueden asignar funciones durante la creación de usuarios. Las funciones determinan el nivel de acceso a los ajustes del dispositivo y a las funciones de administración de dispositivos. El control de acceso basado en el alcance (SBAC) es una extensión de la función de RBAC que permite a un administrador restringir una función de Administrador de dispositivos a un subconjunto de grupos de dispositivos denominado alcance.

Durante la creación o actualización de un usuario con la función Administrador de dispositivos (DM), los administradores pueden asignar un alcance para restringir el acceso operativo del DM a uno o más grupos de sistemas, grupos personalizados o grupos de plug-ins.

Las funciones Administrador y Lector tienen alcance sin restricciones. Esto significa que tienen acceso operativo según lo especificado en los privilegios de RBAC a todas las entidades de dispositivos y grupos.

El alcance puede implementarse de la siguiente manera:

1. Crear o editar usuario
2. Asignar función de DM
3. Asignar el alcance para restringir el acceso operativo

Para obtener más información acerca de la administración de usuarios, consulte Administración de usuarios de OpenManage Enterprise en la página 147.

Cuando un usuario con la función Administrador de dispositivos (DM) y con un alcance asignado inicia sesión, el DM solo puede ver y administrar dispositivos que se encuentren dentro de su alcance. Además, el DM puede ver y administrar entidades, como trabajos, líneas de base y plantillas de firmware o configuración, políticas de alerta, perfiles, etc., que estén asociadas con los dispositivos dentro del alcance, solo si el DM es propietario de la entidad (el DM creó esa entidad o se le asignó la propiedad). Para obtener más información acerca de las entidades que puede crear un DM, consulte *Privilegios de control de acceso basado en funciones (RBAC) en OpenManage Enterprise*.

Por ejemplo, cuando hace clic en **Configuración** > **Plantillas**, un usuario con la función DM puede ver las plantillas predeterminadas y personalizadas que le pertenecen al DM. Además, el DM puede realizar otras tareas si en el RBAC se le otorgan privilegios para las plantillas que le pertenecen.

Si hace clic en **Configuración** > **Pools de identidades**, el DM puede ver todas las identidades que creó un administrador o el DM. El DM también puede realizar acciones en las identidades especificadas por los privilegios de RBAC. Sin embargo, el DM solo puede ver el uso de las identidades que están asociadas a los dispositivos dentro del alcance del DM.

Del mismo modo, si hace clic en **Configuración** > **Pools de VLAN**, el DM puede ver y exportar todas las VLAN que creó el administrador. El DM no puede realizar ninguna otra operación. Si el DM tiene una plantilla, la puede editar para utilizar las redes VLAN, pero no puede editar la red VLAN.

En OpenManage Enterprise, el alcance se puede asignar durante la creación local o importación de un usuario de AD/LDAP. La asignación del alcance a usuarios de OIDC solo se puede realizar en proveedores de Open ID Connect (OIDC).

SBAC para usuarios locales:

Cuando crea o edita un usuario local con la función de DM, el administrador puede seleccionar uno o más grupos de dispositivos que definen el alcance del DM.

Por ejemplo, usted (como administrador) crea un DM llamado dm1 y asigna el grupo *g1* presente en grupos personalizados. Entonces, dm1 solo tendrá acceso operativo a todos los dispositivos en *g1*. El usuario dm1 no podrá acceder a ningún otro grupo o entidad relacionada con otros dispositivos.

Además, con SBAC, dm1 tampoco podrá ver las entidades que cree otro DM (por ejemplo, dm2) en el mismo grupo *g1*. Esto significa que un DM solo podrá ver las entidades que le pertenecen a su usuario.

Por ejemplo, usted (como administrador) crea otro DM llamado dm2 y asigna el mismo grupo *g1* presente en grupos personalizados. Si dm2 crea una plantilla de configuración, líneas de base de configuración o perfiles para los dispositivos en *g1*, el dm1 no tendrá acceso a esas entidades, y viceversa.

Un DM con el alcance Todos los dispositivos tiene acceso operativo según lo especificado en los privilegios de RBAC para todos los dispositivos y las entidades de grupo que le pertenecen al DM.

SBAC para usuarios de AD/LDAP:

Durante la importación o edición de grupos de AD/LDAP, los administradores pueden asignar alcances para grupos de usuarios con la función de DM. Si un usuario es miembro de varios grupos de AD, cada uno con una función de DM, y cada grupo de AD tiene distintas asignaciones de alcance, el alcance del usuario es la combinación de los alcances de esos grupos de AD.

Por ejemplo,

- El usuario dm1 es miembro de dos grupos de AD (*RR5-Floor1-LabAdmins* y *RR5-Floor3-LabAdmins*). Ambos grupos de AD tienen asignada la función de DM, y las asignaciones de alcance para los grupos de AD son las siguientes: *RR5-Floor1-LabAdmins* obtiene *ptlab-servers* y *RR5-Floor3-LabAdmins* obtiene *smdlab-servers*. Ahora, el alcance del DM dm1 es la combinación de *ptlab-servers* y *smdlab-servers*.
- El usuario dm1 es miembro de dos grupos de AD (*adg1* y *adg2*). Ambos grupos de AD tienen asignada la función de DM, con asignaciones de alcance para los grupos de AD como se indica a continuación: *adg1* recibe acceso a *g1* y *adg2* recibe acceso a *g2*. Si *g1* es el supraconjunto de *g2*, el alcance de dm1 es el alcance mayor (*g1*, todos sus grupos secundarios y todos los dispositivos inferiores).

Cuando un usuario es miembro de varios grupos de AD que tienen diferentes funciones, la de mayor funcionalidad tiene prioridad (en el orden Administrador, DM, Lector).

Un DM con acceso sin restricciones tiene acceso operativo según lo especificado en los privilegios de RBAC a todas las entidades de dispositivos y grupos.

NOTA: Después de actualizar OpenManage Enterprise a la versión 3.6, los administradores de dispositivos AD/LDAP y OIDC (PingFederate o KeyCloak) deben volver a crear todas las entidades de la versión anterior, ya que estas entidades solo están disponibles para los administradores después de la actualización. Para obtener más información, consulte las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC para usuarios de OIDC:

La asignación de alcance para usuarios de OIDC no se realiza en la consola de OME. Puede asignar alcances para usuarios de OIDC en un proveedor de OIDC durante la configuración de usuario. Cuando el usuario inicie sesión con las credenciales del proveedor de OIDC, la asignación de la función y el alcance estará disponible para OME. Para obtener más información acerca de la configuración de las funciones y los alcances de usuario, consulte Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160.

NOTA: Si se utiliza PingFederate como el proveedor de OIDC, solo se pueden usar las funciones de administrador. Para obtener más información, consulte Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160 y las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transferir propiedad: El administrador puede transferir recursos de a un administrador de dispositivos (fuente) a otro administrador de dispositivos. Por ejemplo, un administrador puede transferir todos los recursos asignados del dm1 de fuente al dm2. Un administrador de dispositivos que sea propietario de entidades, como líneas de base de firmware o configuración, plantillas de configuración, políticas de alerta y perfiles, se considera un usuario de fuente elegible. La transferencia de propiedad se realiza solo con las entidades y no los grupos de dispositivos (alcance) que son propiedad de un administrador de dispositivos a otro. Para obtener más información, consulte Transferir la propiedad de entidades de administrador de dispositivos en la página 154.

Referencias relacionadas

Tipos de roles de usuario en OpenManage Enterprise en la página 15

Tareas relacionadas

Instalar OpenManage Enterprise en la página 20

3

Instalar OpenManage Enterprise

Dell EMC OpenManage Enterprise se proporciona como un dispositivo que puede instalar en un hipervisor y permite administrar recursos para minimizar el tiempo de inactividad. El servidor virtual se puede configurar desde la consola web de aplicaciones después del aprovisionamiento inicial de la red en la interfaz de usuario de texto (TUI). Para conocer los pasos para ver y actualizar la versión de la consola, consulte Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167. En este capítulo se describen los requisitos previos y mínimos para la instalación.

NOTA: Para obtener más información sobre los navegadores compatibles, consulte la *Matriz de soporte de OpenManage Enterprise* disponible en el sitio de soporte técnico.

Referencias relacionadas

Tipos de roles de usuario en OpenManage Enterprise en la página 15
Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise en la página 35
Características de seguridad en OpenManage Enterprise en la página 15

Información relacionada

Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Temas:

Prerrequisitos de instalación y requisitos mínimos

Para obtener una lista de las plataformas, los sistemas operativos y los navegadores admitidos, consulte la *Matriz de soporte Dell EMC OpenManage Enterprise* en el sitio de soporte técnico y en Dell TechCenter.

Para instalar OpenManage Enterprise, debe tener derechos de administrador del sistema local y el sistema que esté utilizando debe cumplir con los criterios que se mencionan en Requisitos mínimos de hardware recomendados y Requisitos mínimos del sistema para instalar OpenManage Enterprise.

Requisitos mínimos recomendados de hardware

Esta tabla describe los requisitos mínimos de hardware recomendados para OpenManage Enterprise.

Tabla 4. Requisitos mínimos recomendados de hardware

Requisitos mínimos recomendados de hardware	Implementaciones amplias	Implementaciones pequeñas
Cantidad de dispositivos que el dispositivo puede administrar	Hasta 8000	1000
RAM	32 GB	16 GB
Procesadores	8 núcleos en total	4 núcleos en total

Tabla 4. Requisitos mínimos recomendados de hardware (continuación)

Requisitos mínimos recomendados de hardware	Implementaciones amplias	Implementaciones pequeñas
Unidad de disco duro	400 GB	400 GB

Requisitos mínimos del sistema para implementar OpenManage Enterprise

Tabla 5. Requisitos mínimos

Detalles	Requisitos mínimos

Hipervisores compatibles	• Versiones de VMware vSphere:
	  ○ vSphere ESXi 5.5 en adelante
	• Microsoft Hyper-V compatible en:
	  ○ Windows Server 2012 R2 en adelante
	• KVM compatible en:
	  ○ Red Hat Enterprise Linux 6.5 en adelante

Red	NIC virtual disponible que tiene acceso a las redes de administración de todos los dispositivos administrados desde OpenManage Enterprise.
Navegadores compatibles	• Internet Explorer (64 bits) 11 y versiones posteriores • Mozilla Firefox 52 y versiones posteriores • Google Chrome 58 y versiones posteriores • Microsoft Edge versión 41.16299 y versiones posteriores
Interfaz de usuario	HTML 5, basado en JS

NOTA: Para ver la actualización más reciente de los requisitos mínimos para OpenManage Enterprise, consulte *Matriz de soporte de Dell EMC OpenManage Enteprise* en el sitio de soporte.

Implementar OpenManage Enterprise en VMware vSphere

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.

1. Descargue el archivo `openmanage_enterprise_ovf_format.zip` desde el sitio de soporte y extraiga el archivo en una ubicación a la que VMware vSphere Client pueda acceder. Se recomienda utilizar una unidad local o un CD/DVD, porque la instalación desde una ubicación de red puede tardar hasta 30 minutos.
2. En el cliente de vSphere, seleccione **Archivo** > **Implementar plantilla OVF**.
   Aparecerá el asistente para **Implementar plantilla OVF**.
3. En la página de **Origen**, haga clic en **Examinar** y, a continuación, seleccione el paquete OVF. Haga clic en **Siguiente**.
4. En la página **Detalles de plantilla OVF**, revise la información que se muestra. Haga clic en **Siguiente**.
5. En la página **Acuerdo de licencia para el usuario final**, lea el acuerdo de licencia y haga clic en **Aceptar**. Para continuar, haga clic en **Siguiente**.
6. En la página **Nombre y ubicación**, ingrese un nombre de hasta 80 caracteres y, a continuación, seleccione una ubicación de inventario donde se debe almacenar la plantilla. Haga clic en **Siguiente**.
7. En función de la configuración de vCenter, aparecerá una de las siguientes opciones:

- **Si se han configurado bloques de recursos**: en la página **Bloque de recursos**, seleccione el bloque de dispositivos virtuales para implementar la aplicación VM.
- **Si NO se han configurado bloques de recursos**: en la página **Hosts o clústeres**, seleccione el host o el clúster en el que desea implementar la máquina virtual del dispositivo.

8. Si hay más de un almacén de datos disponible en el host, en la página **Almacén de datos** se muestran esos almacenes de datos. Seleccione la ubicación para almacenar los archivos de máquinas virtuales (VM) y, a continuación, haga clic en **Siguiente**.
9. En la página **Formato de disco**, haga clic en **Aprovisionamiento grueso** para preasignar espacio físico de almacenamiento a máquinas virtuales en el momento en que se crea una unidad.
10. En la página **Listo para completar**, revise las opciones que seleccionó en las páginas anteriores y haga clic en **Finalizar** para ejecutar el trabajo de implementación.
    De este modo, se muestra una ventana del estado de finalización donde puede realizar un seguimiento del trabajo de detección.

Implementar OpenManage Enterprise en Hyper-V 2012 R2 y host anteriores

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.
- Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.

1. Descargue el archivo `openmanage_enterprise_vhd_format.zip` desde el sitio de soporte. Extraiga el archivo y, a continuación, mueva o copie el archivo VHD adjunto a la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
2. Inicie el **Administrador de Hyper-V** en Windows Server 2012 R2 o en una versión anterior. Windows Hyper-V debe aparecer en el administrador de Hyper-V. Si no es así, haga clic con el botón secundario en **Administrador de Hyper-V** y seleccione **Conectar al servidor**.
3. Haga clic en **Acciones** > **Nueva** > **Máquina virtual** para iniciar el **Asistente de nueva máquina virtual**.
4. Haga clic en **Siguiente** en la página inicial **Antes de comenzar**.
5. En la **página Especificar nombre y ubicación**,
   - proporcione el **Nombre de la máquina virtual.**
   - (Opcional) Seleccione la casilla de verificación **Almacenar la máquina virtual en una ubicación diferente** para activar el campo **Ubicación** y, a continuación, navegue para capturar una ubicación de la carpeta en la que se almacena la VM.

   NOTA: Si no está seleccionada la casilla de verificación, la máquina virtual se almacena en la carpeta predeterminada.
6. Haga clic en **Siguiente**.
7. En la página **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.

   NOTA: OpenManage Enterprise no es compatible con la 2.ª generación.
8. En la página **Asignar memoria**, ingrese la memoria de inicio en el campo **Memoria de inicio** y haga clic en **Siguiente**.

   NOTA: Asegúrese de que se asigne un mínimo de 16 000 MB (16 GB).
9. En la página **Configurar redes,** seleccione el adaptador de red en la lista desplegable **Conexión**. Asegúrese de que el **Switch virtual** esté conectado a la red. Haga clic en **Siguiente**.

   NOTA: Si se establece en "**No Conectado**", OME no funcionará correctamente durante el primer reinicio y es necesario implementarlo nuevamente, si vuelve a ocurrir esta situación.
10. En la página **Conectar disco duro virtual,** seleccione **Usar una unidad de disco virtual existente** y, a continuación, navegue a la ubicación en la que se copió el archivo VHD como se indica en el **paso 1**. Haga clic en **Siguiente**.
11. Complete las instrucciones que aparecen en pantalla.

    NOTA: Asegúrese de tener un tamaño de almacenamiento mínimo de 20 GB
12. Abra la **Configuración** de la nueva MV creada y encienda la VM.

13. En la pantalla TUI, acepte el EULA y, cuando se le indique, cambie la contraseña del dispositivo y establezca los parámetros de red para la IP del dispositivo.

Implementar OpenManage Enterprise en un host de Hyper-V 2016

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.
- Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.

1. Descargue el archivo **openmanage_enterprise_vhd_format.zip** desde el sitio de soporte. Extraiga el archivo y, a continuación, mueva o copie el archivo VHD adjunto a la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
2. Inicie el **Administrador de Hyper-V** en Windows Server 2016. Windows Hyper-V debe aparecer en el administrador de Hyper-V. Si no es así, haga clic con el botón secundario en **Administrador de Hyper-V** y seleccione **Conectar al servidor**.
3. Haga clic en **Acciones** > **Nueva** > **Máquina virtual** para iniciar el **Asistente de nueva máquina virtual**.
4. Haga clic en **Siguiente** en la página inicial **Antes de comenzar**.
5. En la **página Especificar nombre y ubicación**,
   - proporcione el **Nombre de la máquina virtual.**
   - (Opcional) Seleccione la casilla de verificación **Almacenar la máquina virtual en una ubicación diferente** para activar el campo **Ubicación** y, a continuación, navegue para capturar una ubicación de la carpeta en la que se almacena la VM.

   NOTA: Si no está seleccionada la casilla de verificación, la máquina virtual se almacena en la carpeta predeterminada.
6. Haga clic en **Siguiente**.
7. En la página **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.

   NOTA: OpenManage Enterprise no es compatible con la 2.ª generación.
8. En la página **Asignar memoria**, ingrese la memoria de inicio en el campo **Memoria de inicio** y haga clic en **Siguiente**.

   NOTA: Asegúrese de que se asigne un mínimo de 16 000 MB (16 GB).
9. En la página **Configurar redes,** seleccione el adaptador de red en la lista desplegable **Conexión**. Asegúrese de que el **Switch virtual** esté conectado a la red. Haga clic en **Siguiente**.

   NOTA: Si se establece en "**No Conectado**", OME no funcionará correctamente durante el primer reinicio y es necesario implementarlo nuevamente, si vuelve a ocurrir esta situación.
10. En la página **Conectar disco duro virtual,** seleccione **Usar una unidad de disco virtual existente** y, a continuación, navegue a la ubicación en la que se copió el archivo VHD como se indica en el **paso 1**. Haga clic en **Siguiente**.
11. Complete las instrucciones que aparecen en pantalla.

    NOTA: Asegúrese de tener un tamaño de almacenamiento mínimo de 20 GB
12. Abra la **Configuración** de la nueva MV creada y encienda la VM.
13. En la pantalla TUI, acepte el EULA y, cuando se le indique, cambie la contraseña del dispositivo y establezca los parámetros de red para la IP del dispositivo.

Implementar OpenManage Enterprise en un host de Hyper-V 2019

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.
- Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.

1. Descargue el archivo **openmanage_enterprise_vhd_format.zip** desde el sitio de soporte. Extraiga el archivo y, a continuación, mueva o copie el archivo VHD adjunto a la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
2. Inicie el **Administrador de Hyper-V** en Windows Server 2019. Windows Hyper-V debe aparecer en el administrador de Hyper-V. Si no es así, haga clic con el botón secundario en **Administrador de Hyper-V** y seleccione **Conectar al servidor**.
3. Haga clic en **Acciones** > **Nueva** > **Máquina virtual** para iniciar el **Asistente de nueva máquina virtual**.
4. Haga clic en **Siguiente** en la página inicial **Antes de comenzar**.
5. En la **página Especificar nombre y ubicación**,
   - proporcione el **Nombre de la máquina virtual.**
   - (Opcional) Seleccione la casilla de verificación **Almacenar la máquina virtual en una ubicación diferente** para activar el campo **Ubicación** y, a continuación, navegue para capturar una ubicación de la carpeta en la que se almacena la VM.

   NOTA: Si no está seleccionada la casilla de verificación, la máquina virtual se almacena en la carpeta predeterminada.
6. Haga clic en **Siguiente**.
7. En la página **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.

   NOTA: OpenManage Enterprise no es compatible con la 2.ª generación.
8. En la página **Asignar memoria**, ingrese la memoria de inicio en el campo **Memoria de inicio** y haga clic en **Siguiente**.

   NOTA: Asegúrese de que se asigne un mínimo de 16 000 MB (16 GB).
9. En la página **Configurar redes,** seleccione el adaptador de red en la lista desplegable **Conexión**. Asegúrese de que el **Switch virtual** esté conectado a la red. Haga clic en **Siguiente**.

   NOTA: Si se establece en "**No Conectado**", OME no funcionará correctamente durante el primer reinicio y es necesario implementarlo nuevamente, si vuelve a ocurrir esta situación.
10. En la página **Conectar disco duro virtual,** seleccione **Usar una unidad de disco virtual existente** y, a continuación, navegue a la ubicación en la que se copió el archivo VHD como se indica en el **paso 1**. Haga clic en **Siguiente**.
11. Complete las instrucciones que aparecen en pantalla.

    NOTA: Asegúrese de tener un tamaño de almacenamiento mínimo de 20 GB
12. Abra la **Configuración** de la nueva MV creada y encienda la VM.
13. En la pantalla TUI, acepte el EULA y, cuando se le indique, cambie la contraseña del dispositivo y establezca los parámetros de red para la IP del dispositivo.

Implementación de OpenManage Enterprise utilizando una máquina virtual basada en kernel

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.

1. Instale los paquetes de virtualización requeridos mientras instala el sistema operativo.
2. Descargue el archivo `openmanage_enterprise_kvm_format.zip` desde el sitio de soporte. Descargue el archivo en la ubicación correspondiente del sistema en la que desee almacenar la unidad virtual OpenManage Enterprise.
3. Inicie el administrador virtual y seleccione **Archivo** > **Propiedades**.

4. En la página **Interfaces de red**, haga clic en **Agregar**.
5. Seleccione **Puente** como tipo de interfaz y haga clic en **Reenviar**.
6. Configure el modo de inicio como **en arranque** y seleccione la casilla de verificación **Activar ahora**.
7. Seleccione la interfaz que va a conectar desde la lista, asegúrese de que las propiedades coinciden con el dispositivo de host y, luego, haga clic en **Finalizar**.
   Se acaba de crear una interfaz virtual y puede configurar la configuración del firewall usando el terminal.
8. En el administrador de máquina virtual, haga clic en **Archivo** > **Nuevo**.
9. Ingrese un nombre para la máquina virtual, seleccione la opción **Importar imagen de disco existente** y haga clic en **Reenviar**.
10. Vaya al sistema de archivos y seleccione el archivo QCOW2 que se descargó en el paso 1. Luego, haga clic en **Reenviar**.
11. Asigne 16 GB como la memoria y seleccione dos núcleos de procesador. A continuación, haga clic en **Reenviar**.
12. Asigne el espacio en disco necesario para la máquina virtual y haga clic en **Reenviar**.
13. En **Opciones avanzadas**, asegúrese de que la red del dispositivo host con puente está seleccionada y de que el Tipo de virtualización seleccionado sea KVM.
14. Haga clic en **Finalizar**.
    El dispositivo OpenManage Enterprise ya está implementado usando el KVM. Para comenzar a utilizar OpenManage Enterprise, consulte Iniciar sesión en OpenManage Enterprise en la página 27.

Implementar mediante programación OpenManage Enterprise

OpenManage Enterprise se puede implementar mediante programación (con un script) en VMware ESXi, versión 6.5 o posterior.

NOTA: La implementación programática o con script solo es compatible mediante el uso de la interfaz principal.

NOTA: Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como **DESHABILITADO** y el usuario deberá configurarlo.

NOTA: Para la implementación programática, debe utilizar las versiones más recientes de la Herramienta OVF y Python 3.0 o posteriores.

Para implementar mediante programación OpenManage Enterprise, realice lo siguiente:

1. Descargue y extraiga el archivo `openmanage_enterprise_ovf_format.zip` o descargue los siguientes archivos OVF individualmente desde el sitio de soporte:
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`
   - `openmanage_enterprise.x86_64-0.0.1.ovf`
   - `openmanage_enterprise.x86_64-0.0.1.vmx`
   - `ovf_properties.config`
   - `update_ovf_property.py`
2. Abra `ovf_properties.config` y configure los siguientes parámetros:

Tabla 6. Parámetros que se usan en `ovf_properties.config`

Parámetro	Valores aceptables	Descripción
bEULATxt	verdadero o falso	Si configura este valor como verdadero, acepta los términos y condiciones del acuerdo de licencia del usuario final (EULA). El EULA está disponible al final del archivo ovf_properties.config.
adminPassword	Debe contener al menos un carácter en: mayúscula, minúscula, dígito y carácter especial. Por ejemplo, Dell123$	Escriba una nueva contraseña de administrador para OpenManage Enterprise.

Tabla 6. Parámetros que se usan en `ovf_properties.config` (continuación)

Parámetro	Valores aceptables	Descripción
bEnableDHCP	verdadero o falso	Establezca como verdadero, si desea que el dispositivo habilite IPv4 DHCP y para omitir la IPv4 estática.
bEnableIpv6AutoConfig	verdadero o falso	Configure como verdadero, si desea que el dispositivo habilite la configuración automática de IPv6 y para omitir la IPv6 estática.
staticIP	IP estática en formato CIDR	Puede ser IPv4 o IPv6. (No puede configurar al mismo tiempo los tipos IPv4 e IPv6).
gateway	IPv4 o IPv6	No puede configurar al mismo tiempo la puerta de enlace estática como tipos IPv4 e IPv6.

3. Ejecute el script `update_ovf_property.py`.

   Este script modifica el archivo `openmanage_enterprise.x86_64-0.0.1.ovf` para la implementación de conformidad con los valores establecidos en el archivo ovf_properties.config. Cuando el script finaliza la ejecución, se muestra un ejemplo de comando de la herramienta ovf. Contiene etiquetas como `<DATASTORE>`, `<user>`, `<password>`, `<IP address>` y así sucesivamente, que debe sustituir según el entorno de implementación. Estas configuraciones definen los recursos que se utilizan en el sistema la destino ESXi además de las credenciales y direcciones IP del sistema de destino.

   NOTA: Recuerde sustituir el etiquetado completo, incluido los símbolos < y >.

4. Ejecute el comando de la herramienta ovf que se modificó en el paso anterior.

   NOTA: El comando de la herramienta ovf se debe ejecutar con las marcas --X:injectOvfEnv y --powerOn, ya que se requieren para la implementación programática.

   Después de ejecutar el comando de la herramienta ovf, el manifiesto se valida y comienza la implementación.

4

Introducción a OpenManage Enterprise

Temas:

Iniciar sesión en OpenManage Enterprise

Cuando se inicia el sistema por primera vez en la interfaz de usuario de texto (TUI), se le pedirá que acepte el EULA y, a continuación, que cambie la contraseña del administrador. Si iniciará sesión en OpenManage Enterprise por primera vez, debe establecer las credenciales de usuario a través de la TUI. Consulte Configurar OpenManage Enterprise con interfaz de usuario de texto en la página 27.

PRECAUCIÓN: Si olvida la contraseña del administrador, no podrá recuperarla desde el dispositivo OpenManage Enterprise.

1. Inicie el navegador compatible.
2. En la casilla **Dirección**, ingrese la dirección IP del servidor OpenManage Enterprise.
3. En la página de inicio de sesión, escriba las credenciales de inicio de sesión y, a continuación, haga clic en **Iniciar sesión**.

   NOTA: El nombre de usuario predeterminado es `admin`.

Si está iniciando sesión en OpenManage Enterprise por primera vez, aparece la página **Bienvenido a OpenManage Enterprise**. Haga clic en **Configuración inicial** y complete la configuración básica. Consulte Configurar OpenManage Enterprise en la página 30. Para detectar los dispositivos, haga clic en **Detectar dispositivos**.

NOTA: De manera predeterminada, después de tres intentos de inicio de sesión fallidos, la cuenta de OpenManage Enterprise se bloquea y no puede iniciar sesión hasta que finalice la duración del bloqueo de cuenta. La duración del bloqueo de cuenta es de 900 segundos de forma predeterminada. Para cambiar este período, consulte Establecimiento de las propiedades de seguridad de inicio de sesión en la página 163.

Configurar OpenManage Enterprise con interfaz de usuario de texto

La herramienta de interfaz de usuario de texto (TUI) proporciona una interfaz de texto para cambiar la contraseña del administrador, ver el estado del dispositivo y la configuración de la red, configurar los parámetros de red, activar la solicitud de depuración del servicio de campo, seleccionar la red principal y configurar el dispositivo para la detección automática de los servidores de la red.

Cuando inicia el sistema por primera vez desde la TUI, se le solicita que acepte el Acuerdo de licencia de usuario final (EULA). A continuación, cambie la contraseña del administrador y configure los parámetros de red para el dispositivo y cargue la consola web en un navegador compatible para comenzar. Solo los usuarios con privilegios de administrador de OpenManage pueden configurar OpenManage Enterprise.

En la interfaz TUI, utilice las teclas de flecha o presione la tecla **Tab** para avanzar a la siguiente opción de la TUI y, a continuación, presione **Shift + Tab** para volver a las opciones anteriores. Presione **Intro** para seleccionar una opción. La barra **espaciadora** cambia el estado de una casilla de verificación.

NOTA:

- Para configurar IPv6, asegúrese de que ya esté configurado por un vCenter Server.

- De manera predeterminada, OpenManage Enterprise utiliza la última IP detectada de un dispositivo para realizar todas las operaciones. Para aplicar cualquier cambio de IP, es necesario volver a detectar el dispositivo.

Puede configurar OpenManage Enterprise mediante la TUI. La pantalla TUI tiene las siguientes opciones:

Tabla 7. Opciones de la interfaz de usuario de texto

Opciones	Descripciones
Cambiar la contraseña del administrador	Seleccione la pantalla **Cambiar la contraseña del administrador** para ingresar una nueva contraseña y confírmela. La primera vez, debe cambiar la contraseña en la pantalla TUI.
Ver estado del dispositivo actual	Seleccione **Mostrar estado actual del dispositivo** para ver la dirección URL y el estado del dispositivo. También puede ver los estados de la ejecución de tareas, el procesamiento de eventos, Tomcat, la base de datos y los servicios de supervisión.
Ver la configuración de red actual	Seleccione **Mostrar la configuración de red actual** para ver los detalles de la configuración de IP. En el menú **Elegir adaptador de red**, se enumeran todos los adaptadores de red disponibles. Si hace clic en un adaptador de red, se mostrará su configuración actual.
Establecer el nombre de host de dispositivo	Seleccione **Establecer el nombre de host de dispositivo** para configurar el nombre de host de dispositivo en el DNS. Este campo admite los siguientes caracteres válidos para los nombres de host: alfanumérico (a-z, A-Z, 0-9), puntos (.) y guiones (-). **NOTA:** El uso de puntos designará la información de nombre de dominio. Si la información de DNS del dispositivo se configura de forma estática en lugar de obtener detalles de dominio desde DHCP, debe configurar el hostname utilizando el nombre de dominio calificado (FQDN) para que se pueda completar la información de búsqueda del dominio.
Establecer parámetros del sistema de red	Seleccione **Establecer parámetros de red** para volver a configurar los adaptadores de red. En el menú **Elegir adaptador de red**, se enumeran todos los adaptadores de red disponibles. Seleccione un adaptador de red, vuelva a configurar los parámetros de red y seleccione **Aplicar** para guardar los cambios en la interfaz correspondiente. De forma predeterminada, solo IPv4 está habilitada en la interfaz de red principal con una IP estática privada en el dispositivo. Sin embargo, si se agrega una nueva interfaz de red, tanto IPv4 como IPv6 estarán habilitadas para el alojamiento múltiple. Si el dispositivo OpenManage Enterprise no logra adquirir una dirección IPv6, verifique si el entorno se configuró para que los anuncios de enrutador tengan encendido el bit administrado (M). Network Manager de las distribuciones de Linux actual provoca un error de enlace cuando este bit está encendido, pero DHCPv6 no está disponible. Asegúrese de que DHCPv6 esté activado en la red o desactive la marca administrada para los anuncios del enrutador. **NOTA:** • La configuración DNS solo está disponible en la interfaz de red principal. Si se desea la resolución del DNS en esta interfaz, se deben poder resolver todos los nombres de host mediante el servidor DNS configurado en la interfaz principal.
Seleccionar interfaz de red principal	**Seleccionar interfaz de red principal** le permite designar una red principal.

Tabla 7. Opciones de la interfaz de usuario de texto (continuación)

Opciones	Descripciones
	La selección de una interfaz principal otorga prioridad a la interfaz seleccionada en términos de enrutamiento y se utiliza como la ruta predeterminada. Esta interfaz tendrá la prioridad de enrutamiento en caso de cualquier ambigüedad. También se espera que la interfaz principal sea la interfaz "pública" que habilita la conexión a Internet o la red corporativa. Se aplican diferentes reglas de firewall a la interfaz principal, lo que permite un control de acceso más estricto, como la restricción de acceso por rango de IP. **NOTA:** Si el alojamiento múltiple está habilitado, se puede acceder al dispositivo desde dos redes. En este caso, el dispositivo utiliza la interfaz principal para toda la comunicación externa y cuando se utiliza la configuración del proxy. Para obtener más información sobre el alojamiento múltiple en OpenManage, consulte la documentación técnica sobre la *Ejecución de scripts remotos con Dell EMC OpenManage Enterprise* en el sitio de soporte.
Configurar rutas estáticas	Seleccione **Configurar rutas estáticas** si las redes requieren la configuración de una ruta estática para comunicarse con una subred específica a través de las redes IPv4 e IPv6. **NOTA:** Se admite un máximo de 20 rutas estáticas por interfaz.
Configurar detección iniciada por servidor	Seleccione **Configurar detección iniciada por servidor** para permitir que el dispositivo genere de manera automática los registros necesarios con el servidor DNS configurado. **NOTA:** • Asegúrese de que el dispositivo esté registrado en DNS y que pueda actualizar de forma dinámica los registros. • Los sistemas de destino deben estar configurados para solicitar los detalles de registro de DNS. • Para cambiar el nombre de dominio de DNS, asegúrese de que el registro de DNS dinámico esté activado en el servidor DNS. Además, registrar el dispositivo en el servidor DNS, seleccione la opción **Seguros y no seguros** en Actualizaciones dinámicas.
Configurar tamaño del disco del dispositivo	Seleccione **Configurar tamaño del disco del dispositivo** para analizar la disponibilidad de espacio de disco o de nuevos discos y, luego, asigne el espacio de disco adicional o los discos para el dispositivo si es necesario. **NOTA:** • Se recomienda encarecidamente obtener una instantánea de MV de la consola como respaldo antes de aplicar cualquier cambio en la configuración del disco. • No se admite la adición posterior de espacio en el disco ni la eliminación o reducción del espacio en el disco ampliado. A fin de eliminar un disco agregado recientemente o de anular la ampliación de espacio en un disco existente, debe regresar a una instantánea de VM anterior. • Si el análisis inicial no detecta ningún espacio sin asignar, asigne espacio de disco adicional o discos a la consola de su hipervisor y vuelva a realizar el análisis. • El análisis y la asignación de espacio de disco están limitados a un máximo de cuatro discos.

Tabla 7. Opciones de la interfaz de usuario de texto (continuación)

Opciones	Descripciones
Activar modo Depuración de servicio de campo (FSD)	Seleccione **Activar modo de depuración de servicio de campo (FSD)** para la depuración de la consola. Para obtener más información, consulte Flujo de depuración de servicio de campo en la página 181.
Reiniciar servicios	Seleccione **Reiniciar servicios** con las siguientes opciones para reiniciar los servicios y las redes: ● **Reiniciar todos los servicios** ● **Reiniciar la red**
Configurar registro de depuración	Seleccione **Configurar registro de depuración** utilizando las siguientes opciones: ● **Activar registros de depuración**: se utiliza para recolectar los registros de depuración de las tareas de supervisión de la aplicación, los eventos y el historial de ejecución de tareas. ● **Desactivar registros de depuración**: se utiliza para desactivar los registros de depuración. ● **Activar retención de SCP**: se utiliza para recolectar los archivos .XML de la plantilla. ● **Desactivar retención de SCP**: se utiliza para desactivar la retención de SCP. Puede descargar los registros de depuración haciendo clic en **Supervisión** > **Registros de auditoría** > **Exportar** > **Exportar registros de consola** en OpenManage Enterprise.
Cambiar el diseño del teclado	Seleccione **Cambiar la distribución del teclado** para cambiar la distribución del teclado si es necesario.
Reiniciar el dispositivo	Seleccione **Reiniciar el dispositivo** para reiniciar el dispositivo. **NOTA:** Después de ejecutar un comando para reiniciar los servicios, es posible que la TUI muestre el siguiente mensaje: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].` El problema de bloqueo parcial probablemente se produce como resultado de la sobrecarga del hipervisor. En dichas situaciones, se recomienda tener al menos 16 GB de RAM y una CPU de 8000 MHz reservada para el dispositivo OpenManage Enterprise. Además, se recomienda reiniciar el dispositivo OpenManage Enterprise cuando aparezca este mensaje.

Configurar OpenManage Enterprise

Si va a iniciar sesión, por primera vez, en OpenManage Enterprise, se muestra la página **Bienvenido a OpenManage Enterprise** que le permite configurar la hora (de forma manual o mediante la sincronización de la hora NTP) además de las configuraciones de proxy.

1. Para configurar manualmente la hora, realice lo siguiente en la sección **Configuración de hora**:
   - Utilice el menú desplegable **Zona horaria** para seleccionar la zona horaria correspondiente.
   - En el cuadro **Fecha**, ingrese o seleccione una fecha.
   - En el cuadro **Hora**, complete la hora.
   - Haga clic en **Aplicar** para guardar la configuración.
2. Si desea utilizar el servidor NTP para sincronizar la hora, haga lo siguiente en la sección **Configuración de hora**:

   NOTA: Cuando se actualiza la configuración del servidor NTP, se cierran automáticamente las sesiones de los usuarios actualmente conectados a OpenManage Enterprise.

   - Seleccione la casilla de verificación **Usar NTP**.

- Para la sincronización de la hora, ingrese la dirección IP o el nombre de host en **Dirección principal de servidor NTP** y **Dirección secundaria de servidor NTP** (opcional)

3. Si desea establecer el servidor proxy para comunicación externa, en la sección Configuración del proxy, haga lo siguiente:
   - Seleccione la casilla de verificación **Habilitar configuración de proxy HTTP**.
   - Ingrese la **Dirección proxy**.
   - Ingrese el **Número del puerto** para el servidor proxy.
   - Si el servidor proxy requiere credenciales para iniciar sesión, seleccione la casilla de verificación **Habilitar autenticación de proxy** y, a continuación, ingrese el nombre de usuario y la contraseña.
   - Seleccione la casilla de verificación **Ignorar validación del certificado** si el proxy configurado intercepta el tráfico SSL y no usa ningún certificado de confianza de otros fabricantes. Si se usa esta opción, se omitirán las comprobaciones incorporadas del certificado, que se utilizan para la sincronización de la garantía y el catálogo.
4. Haga clic en **Aplicar** para guardar la configuración.

NOTA: Para obtener más información sobre los navegadores compatibles, consulte la *Matriz de soporte de OpenManage Enterprise* disponible en el sitio de soporte técnico.

Configuración recomendada de escalabilidad y rendimiento para el uso óptimo de OpenManage Enterprise

En la siguiente tabla se muestran los parámetros de rendimiento de las funciones compatibles en OpenManage Enterprise. Para garantizar un rendimiento óptimo de OpenManage Enterprise, Dell EMC recomienda ejecutar las tareas con la frecuencia especificada en el número máximo de dispositivos que se recomienda por tarea.

Tabla 8. Consideraciones de escalabilidad y rendimiento de OpenManage Enterprise

Tareas	Frecuencia recomendada para ejecutar las tareas	¿Están predefinidas las tareas?	Número máximo de dispositivos recomendados por tarea.
Detección	Una vez al día para entornos con cambios de red frecuentes.	No	10.000/tarea
Inventario	OpenManage Enterprise ofrece una tarea predefinida que actualiza automáticamente el inventario una vez al día.	Sí. Puede desactivar esta función.	Dispositivos supervisados por OpenManage Enterprise.
Garantía	OpenManage Enterprise ofrece una tarea predefinida que actualiza automáticamente la garantía una vez al día.	Sí. Puede desactivar esta función.	Dispositivos supervisados por OpenManage Enterprise.
Sondeo de la condición	Cada una hora	Sí. Puede cambiar la frecuencia.	Not applicable
Actualizar el firmware o los controladores	Según sea necesario		150 por tarea
Inventario de configuración	Según sea necesario		1500 por base

Protocolos y puertos admitidos en OpenManage Enterprise

Protocolos y puertos admitidos en Management Stations

Tabla 9. Protocolos y puertos admitidos por OpenManage Enterprise en estaciones de administración

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
22	SSH	TCP	256 bits	Estación de administración	Entrada	Dispositivo OpenManage Enterprise	• Se requiere para entrante solo si se utiliza FSD. El administrador de OpenManage Enterprise debe activarlo solo si va a interactuar con el personal de asistencia de Dell EMC.
25	SMTP	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	• Para recibir alertas de OpenManage Enterprise por correo electrónico.
53	DNS	UDP/TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	• Para realizar consultas DNS.
68/546 (IPv6)	DHCP	UDP/TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	• Configuración de red.
80*	HTTP	TCP	Ninguno	Estación de administración	Entrada	Dispositivo OpenManage Enterprise	• La página principal de la interfaz gráfica de usuario web. Esto redirigirá a un usuario a HTTPS (puerto 443).
123	NTP	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Servidor NTP	• Sincronización de hora (si está activada).
137, 138, 139, 445	CIFS	UDP/TCP	Ninguno	IDRAC/CMC	Entrada	Dispositivo OpenManage Enterprise	• Para cargar o descargar plantillas de implementación. • Para cargar TSR y los registros de diagnóstico. • Para descargar los DUP de firmware/ controlador y el proceso FSD. • Arrancar en el ISO de red.
				Dispositivo OpenManage Enterprise	Salida	Recurso compartido de CIFS	• Para importar catálogos de firmware o

Tabla 9. Protocolos y puertos admitidos por OpenManage Enterprise en estaciones de administración (continuación)

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
							controladores desde el recurso compartido CIFS.
111, 2049 (valor predeterminado)	NFS	UDP/TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Recurso compartido de NFS externo	• Para descargar el catálogo y los DUP desde el recurso compartido de NFS para las actualizaciones de firmware. • Para la actualización manual de la consola desde un recurso compartido de red.
162*	SNMP	UDP	Ninguno	Estación de administración	Entrada/ Salida	Dispositivo OpenManage Enterprise	• Recepción de sucesos mediante SNMP. La dirección es de 'salida' solo si se utiliza la política de reenvío de captura.
443 (valor predeterminado)	HTTPS	TCP	SSL de 128 bits	Estación de administración	Entrada/ Salida	Dispositivo OpenManage Enterprise	• GUI web • Para descargar actualizaciones e información de garantía desde Dell.com. El cifrado de 256 bits se permite cuando se comunica con OpenManage Enterprise mediante HTTPS para la interfaz gráfica de usuario web. • Detección iniciada por servidor.
514	Syslog	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Servidor Syslog	• Para enviar un alerta e información de registros de auditoría al servidor Syslog.
3269	LDAPS	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	• Inicio de sesión AD/ LDAP para catálogo global.
636	LDAPS	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	• Inicio de sesión AD/LDAP para controlador de dominio.

* El puerto se puede configurar hasta 499 sin incluir los números de puerto que ya están asignados.

Protocolos y puertos admitidos en nodos administrados

Tabla 10. Protocolos y puertos admitidos por OpenManage Enterprise en nodos administrados

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
22	SSH	TCP	256 bits	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	• Para la detección de Hyper-V, Linux OS y Windows.
161	SNMP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	• Para hacer consultas SNMP.
162*	SNMP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Entrada/ Salida	Nodo administrado	• Enviar y recibir capturas de SNMP
443	Propio/WS-Man/ Redfish	TCP	256 bits	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	• Detección e inventario de iDRAC7 y versiones posteriores. • Para la administración de CMC.
623	IPMI/ RMCP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	• Acceso a IPMI mediante LAN
69	TFTP	UDP	Ninguno	CMC	Entrada	Estación de administración	• Para actualizar el firmware de CMC.

* El puerto se puede configurar hasta 499 sin incluir los números de puerto que ya están asignados.

NOTA: En un entorno IPv6, debe habilitar IPv6 y deshabilitar IPv4 en el dispositivo OpenManage Enterprise para asegurarse de que todas las funciones se ejecuten de la manera prevista.

Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise

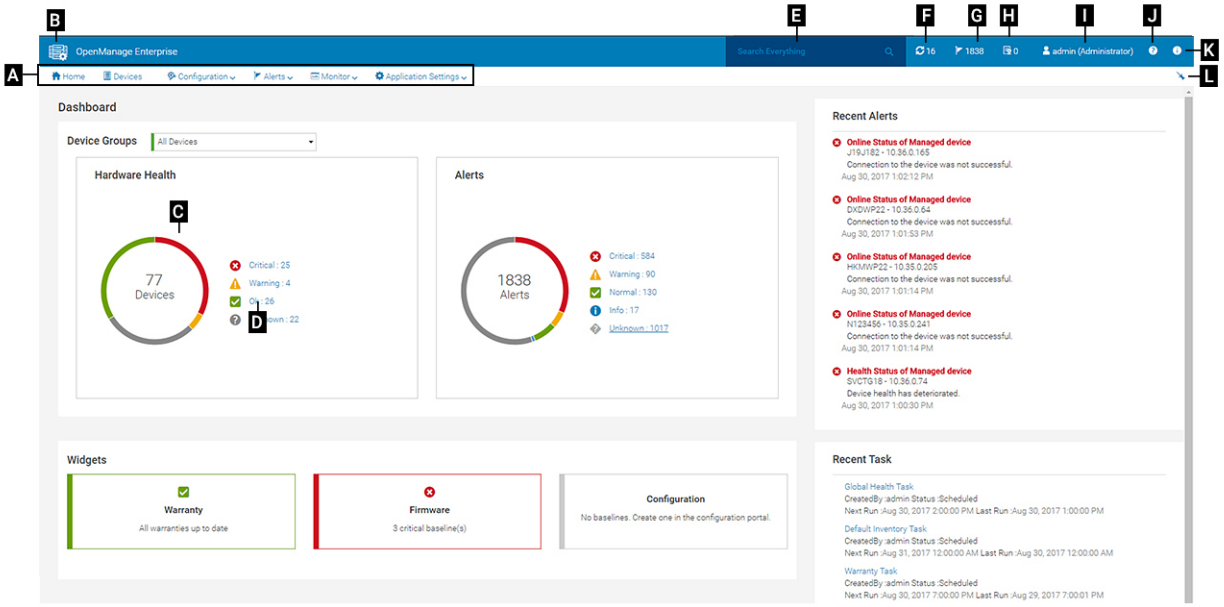
Tabla 11. Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise

Caso de uso	URL
Actualizar dispositivo OpenManage Enterprise	https://downloads.dell.com/openmanage_enterprise/
Acceder a la garantía de dispositivos	https://apigtwb2c.us.dell.com/PROD/sbil/eapi/v5/asset-entitlements
Actualizar catálogos	https://downloads.dell.com/catalog/
Mostrar las nuevas notificaciones de alerta mediante la aplicación OpenManage Mobile	https://openmanagecloud.dell.com

5

Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise

En la interfaz gráfica de usuario (GUI) de OpenManage Enterprise, puede utilizar elementos de menú, vínculos, botones, paneles, cuadros de diálogo, listas, pestañas, casillas de filtrado y páginas para navegar entre páginas y completar las tareas de administración de dispositivos. Las características como la lista de dispositivos, los gráficos de anillo, los registros de auditoría, la configuración de OpenManage Enterprise, las alertas del sistema y la actualización del firmware o los controladores se muestran en más de un lugar. Se recomienda que se familiarice con los elementos de la interfaz gráfica de usuario con el fin de usar OpenManage Enterprise de manera fácil y eficaz para administrar los dispositivos del centro de datos.



- A: el menú **OpenManage Enterprise** en todas las páginas de OpenManage Enterprise proporciona enlaces a las características que permiten a los administradores ver el panel (**Inicio**), administrar los dispositivos (**Dispositivos**), administrar las bases del firmware y los controladores, las plantillas y las bases de cumplimiento de la configuración (**Configuración**), crear y almacenar las alertas (**Alertas**) y, luego, ejecutar trabajos, detectar, recolectar datos de inventario y generar informes (**Supervisión**). También puede personalizar las diversas propiedades de OpenManage Enterprise (**Configuración de la aplicación**). Haga clic en el símbolo de alfiler en la esquina superior derecha para fijar los elementos de menú, de modo que aparezcan en todas las páginas de OpenManage Enterprise. Para quitarlos, nuevamente haga clic en el símbolo de alfiler.
- B: Símbolo del Panel. Haga clic en este símbolo para abrir la página de panel en cualquier página de OpenManage Enterprise. De manera alternativa, haga clic en **Inicio**. Consulte Panel.
- C: el gráfico de anillo proporciona una instantánea del estado de todos los dispositivos supervisados por OpenManage Enterprise. Le permite tomar acciones rápidamente con aquellos dispositivos que se encuentran en estado crítico. Cada color en el gráfico representa un grupo de dispositivos que tienen un estado de condición en particular. Haga clic en las respectivas bandas de colores para ver los dispositivos correspondientes en la lista de dispositivos. Haga clic en el nombre del dispositivo o en una dirección IP para ver la página de propiedades del dispositivo. Consulte Ver y configurar dispositivos individuales en la página 67.
- D: Los símbolos utilizados para indicar el estado de los dispositivos. Consulte Estados de los dispositivos en la página 39.
- E: En el cuadro **Buscar todo**, ingrese lo que esté sujeto a monitoreo y que se pueda mostrar en OpenManage Enterprise para ver los resultados, como la dirección IP del dispositivo, el nombre del trabajo, el nombre del grupo, la línea de base del firmware o los controladores y los datos de la garantía de todos los dispositivos dentro de su alcance, según se define en el Control de acceso basado en el alcance (SBAC). No se puede ordenar ni exportar datos recuperados mediante la función Buscar todo. En los cuadros de diálogo o las páginas individuales, ingrese o seleccione información en la sección **Filtros avanzados** para especificar los resultados de la búsqueda.
    - **No se admiten los siguientes operadores: +, -, y ".**

- F: número de trabajos de OpenManage Enterprise que actualmente se encuentran en la línea de espera. Trabajos relacionados con la detección, el inventario, la garantía y la actualización del firmware o los dispositivos, entre otros. Haga clic para ver el estado de los trabajos que se ejecutan bajo las categorías de Estado, Inventario e Informe en la página Detalles del trabajo. Para ver todos los eventos, haga clic en **Todos los trabajos**. Consulte Utilización de trabajos para el control de dispositivos en la página 128. Haga clic en Actualizar.
- G: número de eventos generados en los registros de alerta. Además, la cantidad de alertas en esta sección varía en función de la configuración para ver o no las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Para ocultar o mostrar la alertas confirmadas, consulte Personalizar la visualización de alertas en la página 165. La eliminación de las alertas reduce la cuenta. Para obtener más información sobre los símbolos que se usan para indicar los estados de gravedad, consulte Estados de los dispositivos en la página 39. Haga clic en un símbolo de gravedad para ver todos los eventos en esa categoría de gravedad en la página Alertas. Para ver todos los servicios, haga clic en **Todos los eventos**. Consulte Administración de alertas de dispositivos.
- H: cantidad total de garantías de dispositivos en estados críticos (vencidas) y de advertencia (que caducan pronto). Consulte Administración de garantía de dispositivos.
- I: nombre del usuario actualmente conectado. Detenga el puntero sobre el nombre de usuario para ver los roles asignados al usuario. Para obtener más información sobre los usuarios basados en el rol, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16. Haga clic para cerrar la sesión y, a continuación, inicie la sesión como un usuario diferente.
- J: actualmente, el archivo de ayuda contextual se muestra solo para la página en que se encuentra y no las páginas de inicio del portal. Haga clic para obtener instrucciones basadas en tareas para utilizar de forma eficaz vínculos, botones, cuadros de diálogo, asistentes y páginas en OpenManage Enterprise.
- K: haga clic en esta opción para ver la versión actual de OpenManage Enterprise instalada en el sistema. Haga clic en **Licencias** para leer el mensaje. Haga clic en los vínculos correspondientes para ver y descargar archivos de código abierto relacionados con OpenManage Enterprise u otras licencias de código abierto.
- L: haga clic en el símbolo para fijar o quitar los elementos de menú. Para fijar elementos de menú, expanda el menú **OpenManage Enterprise** y haga clic en el símbolo de alfiler.

Los datos sobre los elementos que se muestran en una tabla pueden verse en su totalidad, exportarse totalmente o basarse en los elementos seleccionados. Consulte Exportar todos los datos o aquellos seleccionados en la página 66. Cuando se visualizan en texto azul, se puede ver y actualizar la información detallada sobre los elementos en una tabla, la que se abre en la misma ventana o en una página separada. Los datos tabulados se pueden filtrar mediante la característica **Filtros avanzados**. Los filtros varían según el contenido que sea vea. Ingrese o seleccione datos de los campos. Los números o el texto sin completar no mostrarán resultados esperados. Los datos que coinciden con los criterios de filtro aparecen en la lista. Para quitar los filtros, haga clic en **Borrar todos los filtros**.

Para ordenar los datos en una tabla, haga clic en el título de la columna. No se puede ordenar ni exportar datos recuperados mediante la función Buscar todo.

Los símbolos se utilizan para identificar los principales elementos importantes, el panel, el estado de la condición del dispositivo, la categoría de alerta, el estado de cumplimiento del firmware y los controladores, el estado de la conexión y el estado de alimentación, entre otros. Haga clic en los botones para avanzar y retroceder del explorador para navegar por las páginas de OpenManage Enterprise. Para obtener más información sobre los navegadores compatibles, consulte la *Matriz de soporte de Dell EMC OpenManage Enterprise* disponible en el sitio de soporte técnico.

Cuando corresponda, la página se divide en paneles izquierdo, de trabajo y derecho para simplificar la tarea de administración de dispositivos. En caso necesario, se muestran las instrucciones en línea y consejos para el uso de herramientas cuando el puntero se encuentra detenido sobre algún elemento de la GUI.

En el panel derecho se muestra la vista previa sobre el dispositivo, el trabajo, el inventario, la base del firmware o los controladores, la aplicación de administración y la consola virtual, entre otros. Seleccione un elemento en el panel de trabajo y, a continuación, haga clic en **Ver detalles** en el panel derecho para ver la información detallada sobre dicho elemento.

Una vez conectado, todas las páginas se actualizan automáticamente. Si durante los inicios de sesión subsiguientes a la implementación del dispositivo se encuentra disponible una versión actualizada de OpenManage Enterprise, recibirá una alerta para actualizar la versión inmediatamente haciendo clic en **Actualizar**. Los usuarios con todos los privilegios de OpenManage Enterprise (administrador, administrador de dispositivos y observador) pueden ver el mensaje, pero solo un administrador puede actualizar la versión. Un administrador puede optar por obtener el recordatorio más tarde o descartar el mensaje. Para obtener más información acerca de la actualización de la versión de OpenManage Enterprise, consulte Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167.

Para todas las acciones basadas en trabajos de OpenManage Enterprise, cuando se crea o se comienza a ejecutar un trabajo, la esquina inferior derecha muestra el mensaje respectivo. Los detalles de los trabajos se pueden ver en la página **Detalles del trabajo**. Consulte Ver listas de trabajos en la página 128.

Información relacionada

Instalar OpenManage Enterprise en la página 20

6

Portal de inicio de OpenManage Enterprise

Si hace clic en **OpenManage Enterprise** > **Inicio**, aparece la página de inicio de OpenManage Enterprise. En la página de inicio:

- Vea el panel para obtener una instantánea en vivo sobre los estados de la condición de los dispositivos y, a continuación, lleve a cabo acciones, según sea necesario. Consulte Panel.
- Vea las alertas de las categorías Crítico y Advertencia, y resuélvalas. Consulte Administración de alertas de dispositivos.
- La sección de widgets indica los estados consolidados de la garantía, el cumplimiento del firmware o los controladores y el nivel de cumplimiento de la configuración de todos los dispositivos. Para obtener más información sobre las características en Widgets, consulte Monitoreo de dispositivos mediante el panel de OpenManage Enterprise en la página 37. En el panel derecho se muestra una lista de las alertas y tareas recientes generadas por OpenManage Enterprise. Para ver más información sobre una alerta o tarea, haga clic en el título de la alerta o la tarea. Consulte Monitoreo y administración de alertas de dispositivos en la página 117 y Utilización de trabajos para el control de dispositivos en la página 128.
- Si se encuentra disponible una versión actualizada de OpenManage Enterprise, se alerta inmediatamente cuando haya una actualización disponible. Para actualizar, haga clic en **Actualizar**. Para obtener más información acerca de la actualización de la versión de OpenManage Enterprise, consulte Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167.
- En la sección **Alertas recientes** se indican las alertas más recientes generadas por los dispositivos que supervisa OpenManage Enterprise. Haga clic en el título de la alerta para ver información detallada sobre la alerta. Consulte Administración de alertas de dispositivos.
- En la sección **Tareas recientes** se indican las tareas más recientes (trabajos) creadas y ejecutadas. Haga clic en el título de la tarea para ver información detallada sobre el trabajo. Consulte Ver listas de trabajos en la página 128.

NOTA: Si inició sesión como administrador de dispositivos, en el portal de inicio, se muestra información relacionada con el dispositivo o el grupo de dispositivos que le pertenezcan al DM. Además, en la lista desplegable Grupos de dispositivos se muestran solo los grupos de dispositivos en los que el administrador de dispositivos tiene acceso operativo. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Temas:

Monitoreo de dispositivos mediante el panel de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Además del primer inicio de sesión, el panel es la primera página que se ve después de cada inicio de sesión subsiguiente en OpenManage Enterprise.

Para abrir la página Panel en cualquier página de OpenManage Enterprise, haga clic en el símbolo del panel ubicado en la esquina superior izquierda. De manera alternativa, haga clic en **Inicio**.

Con el uso de los datos de supervisión en tiempo real, en el panel se muestra la condición del dispositivo, el cumplimiento del firmware o los controladores, la garantía, las alertas y otros aspectos de los dispositivos y grupos de dispositivos que se encuentran en el entorno del centro de datos.

En el panel también se muestran las actualizaciones disponibles de la consola . Puede actualizar la versión de OpenManage Enterprise inmediatamente o configurar OpenManage Enterprise para que se lo recuerde posteriormente.

De manera predeterminada, cuando se conecta a la aplicación por primera vez, aparece en blanco la página Panel. Agregue dispositivos a OpenManage Enterprise para que se puedan supervisar y mostrar en el panel. Para agregar dispositivos, consulte Detección de dispositivos para la supervisión o administración en la página 40 y Organizar los dispositivos en grupos en la página 54.

- Administrar el firmware y los controladores del dispositivo en la página 75
- Administración de alertas de dispositivos
- Detección de dispositivos
- Creación de informes
- Administración de los ajustes del servidor OpenManage Enterprise en la página 146

NOTA: Si selecciona un grupo de dispositivos en el menú desplegable **Grupos de dispositivos**, en el panel solo se mostrarán datos del grupo de dispositivos seleccionado.

De manera predeterminada, en la sección **Condición del hardware** se muestra un gráfico de anillo que indica la condición actual de todos los dispositivos que se supervisan mediante OpenManage Enterprise. Haga clic en las secciones del gráfico de anillo para ver la información sobre los dispositivos con los respectivos estados de condición.

Un gráfico de anillo en la sección **Alertas** indica las alertas que reciben los dispositivos en los grupos de dispositivos seleccionados. Consulte Monitoreo y administración de alertas de dispositivos en la página 117. La cantidad total de alertas en el gráfico de anillo varía según la configuración de la vista de las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Consulte Personalizar la visualización de alertas en la página 165. Para ver las alertas en cada categoría, haga clic en las bandas respectivas de colores. En el cuadro de diálogo **Alertas**, en la sección Crítico se indican las alertas en estado crítico. Para ver todas las alertas que se han generado, haga clic en **Todos**. La columna **NOMBRE DE ORIGEN** indica el dispositivo que ha generado la alerta. Haga clic en el nombre para ver y configurar las propiedades del dispositivo. Consulte Ver y configurar dispositivos individuales en la página 67.

Para obtener más información sobre un gráfico de anillo, consulte Gráfico de anillo en la página 38 y Estados de los dispositivos en la página 39. Para ver el resumen de los dispositivos en un grupo de dispositivos diferente que se supervisa mediante OpenManage Enterprise, seleccione en el menú desplegable **Grupos de dispositivos**. Para ver la lista de dispositivos que pertenecen a un estado, puede hacer clic en la banda de colores relacionados con una categoría de estado o en el símbolo de estado situado junto al gráfico de anillo.

NOTA: En la lista Dispositivos, haga clic en el nombre del dispositivo o en una dirección IP para ver los datos de configuración del dispositivo y, a continuación, editarlos. Consulte Ver y configurar dispositivos individuales en la página 67.

La sección Widgets proporciona un resumen de algunas de las características clave de OpenManage Enterprise. Para ver un resumen de cada categoría, haga clic en el título del widget.

- **Garantía**: muestra el número de dispositivos cuya garantía está por caducar. Esto se basa en la **Configuración de la garantía**. Si el usuario opta por la notificación de caducidad de la garantía, entonces se muestra la cantidad de dispositivos cuya garantía está vencida. De lo contrario, se muestra la cantidad que caduca pronto o el recuento de las garantías activas. Haga clic para ver más información en el cuadro de diálogo **Garantía**. Para obtener información sobre la administración de la garantía del dispositivo, consulte Administración de la garantía del dispositivo en la página 136. Detenga el puntero del mouse sobre la sección **Garantía** para leer las definiciones sobre los símbolos utilizados en la sección.
- **Firmware/Controladores**: muestra el estado de cumplimiento del firmware o los controladores de las bases de los dispositivos creadas en OpenManage Enterprise. Si están disponibles, en esta sección se muestran las bases de firmware y dispositivos marcadas como críticas y de advertencia.
  - Para obtener más información sobre el estado de resumen, consulte la documentación técnica *ADMINISTRACIÓN DEL ESTADO DE RESUMEN MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.
  - Haga clic para ver más información en la página **Cumplimiento del firmware/controlador**.
  - Para obtener información sobre la actualización de un firmware, la creación del catálogo de firmware, la creación de la línea base de firmware y la generación de un informe de cumplimiento de línea base, consulte Administrar el firmware y los controladores del dispositivo en la página 75.
- **Configuración**: muestra el estado de la condición de las líneas de base de cumplimiento de la configuración creadas en OpenManage Enterprise. Si están disponibles, se muestran las líneas base de configuración críticas y de aviso. Consulte Administrar plantillas de cumplimiento en la página 110.
- **Utilización de recursos**: muestra la utilización de la CPU y la memoria por parte del dispositivo. Las siguientes comprobaciones codificadas por color se utilizan para indicar las diversas etapas de utilización:
  - Verde: una utilización menor que el 80 % del recurso
  - Amarillo: una utilización mayor que el 80 %, pero menor que el 95 % del recurso
  - Rojo: una utilización mayor que el 95 % del recurso

  NOTA: La utilización general del recurso, que se muestra como una barra vertical codificada por color a la izquierda del widget, es la acumulación del peor estado de un recurso.

Gráfico de anillo

Puede ver un gráfico de anillo en diferentes secciones de OpenManage Enterprise. La salida que muestra el gráfico de anillo se basa en los elementos seleccionados en una tabla. El gráfico de anillo indica varios estados en OpenManage Enterprise:

- El estado de los dispositivos: se muestra en la página Panel. Los colores del gráfico de anillo dividen el anillo de forma proporcional para indicar la condición de los dispositivos que supervisa OpenManage Enterprise. El estado de cada dispositivo se indica mediante un símbolo de color. Consulte Estados de los dispositivos en la página 39. Si el gráfico de anillo indica el estado de 279 dispositivos en el grupo, en que el estado de 131 dispositivos es crítico, 50 dispositivos es de advertencia, y 95 dispositivos es correcto, el círculo se forma usando bandas de colores que representan proporcionalmente estos números.

NOTA: El gráfico de anillo de un único dispositivo está formada por un círculo grueso de un solo color que indica el estado del dispositivo. Por ejemplo, en el caso de un dispositivo en el estado Advertencia, se muestra un círculo de color amarillo.

- Estados de alerta de los dispositivos: indican el total de alertas generadas para los dispositivos que supervisa OpenManage Enterprise. Consulte Monitoreo y administración de alertas de dispositivos en la página 117.

  NOTA: La cantidad total de alertas en el gráfico de anillo varía según la configuración de la vista de las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Consulte Personalizar la visualización de alertas en la página 165.

- Para conocer el cumplimiento de la versión de firmware de un dispositivo en comparación con la versión del catálogo, consulte Administrar el firmware y los controladores del dispositivo en la página 75.
- Para conocer la línea base de cumplimiento de la configuración de los dispositivos y grupos de dispositivos, consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

NOTA: El nivel de cumplimiento del dispositivo seleccionado se indica en un gráfico de anillo. Cuando más de un dispositivo está relacionado con una línea base, el estado de un dispositivo con el nivel de cumplimiento más bajo con respecto a la línea base se indica como el mismo nivel de cumplimiento de dicha línea base. Por ejemplo, si varios dispositivos están relacionados con una línea base de firmware y el nivel de cumplimiento de algunos dispositivos es Correcto o Cambiar a una versión anterior , pero si el cumplimiento de un dispositivo en el grupo es Actualizar , el nivel de cumplimiento del firmware de base se indica como Actualizar. El estado de resumen es igual al estado del dispositivo que tiene alta gravedad. Para obtener más información sobre el estado de resumen, consulte la documentación técnica *ADMINISTRACIÓN DEL ESTADO DE RESUMEN MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.

NOTA: El gráfico de anillo de un único dispositivo está formada por un círculo grueso de un solo color que indica el nivel de cumplimiento del firmware del dispositivo. Por ejemplo, para un dispositivo en estado Crítico, aparece un círculo de color rojo que indica que el firmware del dispositivo se debe actualizar.

Estados de los dispositivos

Tabla 12. Estados de los dispositivos en OpenManage Enterprise

Estado de la condición	Definición
Crítico	Indica la incidencia de una falla en un aspecto importante del dispositivo o del entorno.
Advertencia	El dispositivo está por fallar. Indica que algunos aspectos del dispositivo o el medio entorno no son normales. Requiere atención inmediata.
Correcto	El dispositivo está completamente funcional.
Desconocido	El estado del dispositivo es desconocido.

NOTA: Los datos que aparecen en el panel dependen de los privilegios que tenga en OpenManage Enterprise. Para obtener más información sobre los usuarios, consulte Administración de usuarios.

7

Detección de dispositivos para la supervisión o administración

Si hace clic en **OpenManage Enterprise** > **Supervisión** > **Detección**, puede detectar dispositivos en el entorno del centro de datos para administrarlos, mejorar su utilización y disponibilidad de recursos para las operaciones críticas de negocios. En la página **Detección** se muestra la cantidad de dispositivos detectados en la tarea con información sobre el estado del trabajo de detección de ese dispositivo. Los estados de trabajo son En cola, Completo y Detenido. El panel derecho muestra información acerca de la tarea, como el total posible de dispositivos, dispositivo detectado con los tipos de dispositivos y su conteo respectivo, hora de la próxima ejecución si está programada y la última hora de detección. **Ver detalles** en el panel derecho se muestran los detalles del trabajo individual de detección.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Para admitir la detección con credenciales de dominio, OpenManage Enterprise (versión 3.2 en adelante) utiliza el protocolo OpenSSH en lugar del protocolo WSMAN utilizado en las versiones anteriores. Por lo tanto, todos los dispositivos Hyper-V y Windows descubiertos antes de actualizar el dispositivo deben eliminarse y volver a detectar usando sus credenciales de OpenSSH. Consulte la documentación de Microsoft para habilitar OpenSSH en Hyper-V y Windows.
- En las páginas **Programas de detección e inventario**, se indica el estado de un trabajo programado como **En cola** en la columna **ESTADO**. Sin embargo, el mismo estado se indica como **Programado** en la página **Trabajos**.
- De manera predeterminada, OpenManage Enterprise utiliza la última IP detectada de un dispositivo para realizar todas las operaciones. Para aplicar cualquier cambio de IP, es necesario volver a detectar el dispositivo.
- En el caso de los dispositivos de otros fabricantes, es posible que vea entradas duplicadas si la detección se realiza con varios protocolos. Esta duplicación se puede corregir mediante la eliminación de las entradas y la redetección de los dispositivos mediante solo el protocolo IPMI.

Con la característica de detección, puede:

- Ver, agregar y quitar dispositivos de la lista de exclusión global. Consulte Exclusión global de rangos en la página 48.
- Crear, ejecutar, editar, eliminar y detener los trabajos de detección de dispositivos.

Tareas relacionadas

Eliminar un trabajo de detección de dispositivos en la página 53
Visualizar los detalles del trabajo de detección de dispositivos en la página 46
Detener un trabajo de detección de dispositivos en la página 47
Ejecutar un trabajo de detección de dispositivos en la página 47
Especificar el modo de detección para crear un trabajo de detección de servidores en la página 49
Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección en la página 49
Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell en la página 51
Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP en la página 52
Especificar el modo de detección para crear VARIOS trabajos de detección en la página 53
Editar un trabajo de detección de dispositivos en la página 47

Temas:

- Ejecutar un trabajo de detección de dispositivos
- Detener un trabajo de detección de dispositivos
- Especificar varios dispositivos mediante la importación de datos desde el archivo .csv
- Exclusión global de rangos
- Especificar el modo de detección para crear un trabajo de detección de servidores
- Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección
- Especificar el modo de detección para crear un trabajo de detección de chasis
- Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección
- Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell
- Especificar el modo de detección para crear un trabajo de detección de conmutadores de red
- Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPPS: configuración adicional para los protocolos de detección
- Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP
- Especificar el modo de detección para crear VARIOS trabajos de detección
- Eliminar un trabajo de detección de dispositivos

Detectar los servidores automáticamente mediante la función de descubrimiento iniciado por servidor

OpenManage Enterprise permite la detección automática de los servidores que tienen la versión de firmware 4.00.00.00 o posterior de iDRAC. El dispositivo se puede configurar para permitir que estos servidores encuentren automáticamente la consola consultando el DNS e iniciar la detección.

Para una detección iniciada por servidor, se deben cumplir los siguientes requisitos:

- Esta función solo se aplica a los servidores que tengan la versión de firmware 4.00.00.00 o posterior de iDRAC.
- Los servidores deben estar en el mismo dominio o subdominio que OpenManage Enterprise.
- OpenManage Enterprise se debe registrar en el DNS para agregar la información de configuración al DNS mediante TUI. Se recomienda que el DNS permita actualizaciones automáticas desde OpenManage Enterprise.
- Se deben limpiar los registros antiguos de la consola del dispositivo en el DNS, si los hubiera, para evitar que se generen varios anuncios de los servidores.

NOTA: El control de acceso basado en el alcance (SBAC) no afecta a las listas de dispositivos en la página **Monitorear** > **Detección iniciada por servidor** y, en esta página, los administradores de dispositivos verán dispositivos que están fuera de su alcance.

Los siguientes pasos se siguen para realizar una detección automática de servidores en OpenManage Enterprise:

1. Agregue la información de configuración de OpenManage Enterprise en el DNS con uno de los siguientes métodos:
   - TUI: mediante la interfaz de TUI, active la opción **Configurar detección iniciada por servidor**. Para obtener más información, consulte Configurar OpenManage Enterprise con interfaz de usuario de texto en la página 27.
   - Manualmente: agregue los siguientes cuatro registros al servidor DNS en la red para los que está configurada la interfaz en el dispositivo. Asegúrese de reemplazar todas las instancias de `<domain>` o `<subdomain.domain>` con el dominio de DNS correspondiente y el nombre de host del sistema.
     - `<OME hostname>.<domain> 3600 A <OME IP address>`
     - `_dcimprovsrv._tcp.<domain> 3600 PTR ptr.dcimprovsrv._tcp.<domain>`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence`
     - `ptr.dcimprovsrv._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>`

     Para crear los registros con `nsupdate` en Linux, utilice los siguientes comandos:
     - Para crear un registro de nombre de host

       ```
       >update add omehost.example.com 3600 A XX.XX.XX.XX
       ```

     - Para agregar registros para la detección iniciada por servidor

       ```
       >update add _dcimprovsrv._tcp.example.com 3600 PTR ptr.dcimprovsrv._
       tcp.example.com.

       >update add ptr.dcimprovsrv._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/
       ```

```
Actions/DiscoveryConfigService.SignalNodePresence

>update add ptr.dcimprovsrv._tcp.example.com 3600 SRV 0 0 443 omehost.example.com.
```

Para crear los registros con `dnscmd` en un servidor DNS de Windows, utilice los siguientes comandos:

- Para crear un registro de nombre de host

```
>dnscmd <DnsServer> /RecordAdd example.com omehost A XX.XX.XX.XX
```

- Para agregar registros para la detección iniciada por servidor

```
>dnscmd <DnsServer> /RecordAdd example.com _dcimprovsrv._tcp PTR
ptr.dcimprovsrv._tcp.example.com

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp TXT URI=/api/
DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

>dnscmd <DnsServer> /RecordAdd example.com ptr.dcimprovsrv._tcp SRV 0 0 443
omehost.example.com
```

2. De manera predeterminada, la política de detección-aprobación, en el dispositivo, se establece en Automática y los servidores que establecen contacto con la consola se detectan automáticamente. Para cambiar los ajustes, consulte Administración de preferencias de consola en la página 163.
3. Una vez que el dispositivo esté configurado como se mencionó en los pasos anteriores, los servidores podrán iniciar el contacto con OpenManage Enterprise consultando el DNS. El dispositivo verifica los servidores después de asegurarse de que el certificado del cliente de los servidores esté firmado por la autoridad de certificación de Dell.

   NOTA: Si hay cambios en la dirección IP del servidor o en el certificado SSL, el servidor reiniciará el contacto con OpenManage Enterprise.
4. En la página **Supervisión** > **Detección iniciada por servidor**, se muestran los servidores que establecen contacto con la consola. También se enumeran los servidores cuyas credenciales se agregaron a la consola, pero que aún no inician el contacto. Se muestran los siguientes estados de los servidores según las condiciones mencionadas anteriormente:
   - Anunciado: el servidor inicia el contacto con la consola; sin embargo, las credenciales del servidor no se agregan a la consola.
   - Credenciales agregadas: se agregan las credenciales del servidor en la consola; sin embargo, el servidor no ha iniciado contacto con la consola.
   - Listo para detectar: se agregan las credenciales del servidor y el servidor ha iniciado contacto.

     NOTA: El dispositivo activa un trabajo de detección cada 10 minutos para detectar todos los servidores en el estado "Listo para detectar". Sin embargo, si la política de detección-aprobación en el dispositivo se configura como "Manual", el usuario deberá activar manualmente el trabajo de detección para cada servidor. Para obtener más información, consulte Administración de preferencias de consola en la página 163
   - Trabajo enviado para detección: este estado indica que el trabajo de detección se inició de forma automática o manual para el servidor.
   - Detectado: se detecta el servidor y aparece en la página Todos los dispositivos.

En la página **Supervisión** > **Detección iniciada por servidor**, se pueden realizar las siguientes tareas:

1. **Importar**: se utiliza para importar las credenciales de los servidores.
   a. Haga clic en **Importar**.
   b. En el asistente de importación de archivos, haga clic en **Cargar archivo de etiquetas de servicio** para navegar y seleccionar el archivo .csv.

      Para ver un archivo CSV de muestra de las credenciales del servidor, haga clic en **Descargar archivo CSV de muestra**.
   c. Haga clic en **Finalizar**.
2. **Detectar**: se utiliza para detectar manualmente los servidores que tienen el estado "Listo para detectar".
   a. Seleccione los servidores que se muestran en la página Detección iniciada por servidor que se encuentran en el estado "Listo para detectar".
   b. Haga clic en **Detectar**.

   Se activa un trabajo de detección para detectar los servidores. La detección posterior de estos servidores se muestra en la página Todos los dispositivos.
3. **Eliminar**: se utiliza para eliminar los servidores enumerados en la página Detección iniciada por servidor.

a. Seleccione los servidores en la página Detección iniciada por servidor que ya se detectaron y se enumeran en la página Todos los dispositivos.
b. Haga clic en **Eliminar.**

Los servidores se eliminan de la página Detección iniciada por servidor.

NOTA: Las entradas correspondientes a los servidores detectados se depuran automáticamente después de 30 días.

4. **Exportar**: se utiliza para exportar las credenciales del servidor en formato HTML, CSV o PDF.
   a. Seleccione uno o más servidores en la página Detección iniciada por servidor.
   b. Haga clic en **Exportar**.
   c. En el asistente para exportar todo, seleccione cualquiera de los siguientes formatos de archivo: HTML, CSV y PDF.
   d. Haga clic en **Finish** (Finalizar). Se crea un trabajo y los datos se exportan en la ubicación seleccionada.

Crear un trabajo de detección de dispositivos

En los siguientes pasos, se describe cómo iniciar un trabajo de detección de dispositivos en OpenManage Enterprise para detectar los dispositivos en su centro de datos mediante el asistente para Crear trabajo de detección.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Para iniciar la creación del trabajo de detección, puede realizar uno de los siguientes pasos:
   - Haga clic en **Monitorear** > **Detección** > **Crear**.
   - Como alternativa, desde la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), haga clic en el menú desplegable **Detección** y, luego, en **Detectar dispositivos**.
2. En el cuadro de diálogo **Crear trabajo de detección**, se completa el nombre predeterminado del trabajo de inventario. Para cambiarlo, escriba el nombre del trabajo de detección.
   De manera predeterminada, el cuadro de diálogo permite definir las propiedades de dispositivos similares a la vez.
   - Para incluir más dispositivos o intervalos para el trabajo de detección actual, haga clic en **Agregar**. Aparece otro conjunto de los siguientes campos donde se pueden especificar las propiedades de los dispositivos: Tipo, Dirección IP/Nombre de host/Rango y Configuración.

     AVISO: OpenManage Enterprise puede administrar un máximo de 8000 dispositivos. Por lo tanto, no especifique redes grandes que tengan más dispositivos que la cantidad máxima de dispositivos admitidos por OpenManage Enterprise. Es posible que se provoque que el sistema abruptamente deje de responder.

     NOTA: Si se detecta una gran cantidad de dispositivos, no se deben crear varios trabajos de detección mediante una dirección IP individual; en su lugar, de debe utilizar el rango IP de los dispositivos.
   - Para detectar los dispositivos mediante la importación de rangos desde el archivo .csv. Consulte Especificar varios dispositivos mediante la importación de datos desde el archivo .csv en la página 47.
   - Para excluir ciertos dispositivos, quitar dispositivos de exclusión o para ver la lista de dispositivos excluidos detectados, consulte Dispositivos excluidos globalmente de los resultados de detección.
3. En el menú desplegable **Tipo de dispositivo**, para detectar:
   - Un servidor, seleccione **SERVIDOR**. Consulte Especificación del modo de detección para crear un trabajo de detección de servidores.
   - Un chasis, seleccione **CHASIS**. Consulte Especificación del modo de detección para crear un trabajo de detección de chasis.
   - Un dispositivo de almacenamiento Dell EMC o switch de red, seleccione **ALMACENAMIENTO DE DELL** o **SWITCH DE SISTEMA DE RED**. Consulte Especificación del modo de detección para crear un trabajo de detección de almacenamiento, almacenamiento de Dell y switch de red.
   - Para detectar los dispositivos usando varios protocolos, seleccione **VARIOS**. Consulte Especificar el modo de detección para crear VARIOS trabajos de detección en la página 53.
4. En el cuadro **IP/Nombre de host/Rango**, escriba la dirección IP, el nombre de host o el rango de la dirección IP que se va a detectar o incluir. Para obtener más información sobre los datos que puede escribir en este campo, haga clic en el símbolo **i**.

   NOTA:
   - El tamaño del rango se limita a 16.385 (0x4001).
   - También se admiten los formatos de CIDR IPv6 e IPv6.
5. En la sección **Configuración**, escriba el nombre de usuario y la contraseña del protocolo que se utiliza para detectar los rangos.
6. Haga clic en **Configuración adicional** para seleccionar un protocolo diferente y cambiar la configuración.

7. En la sección **Programación de un trabajo de detección**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos en la página 179.
8. Seleccione **Habilitar recepción de captura de servidores iDRAC y chasis MX7000 detectados** para permitir que OpenManage Enterprise reciba las capturas entrantes desde los servidores y los chasis MX7000 detectados.

   NOTA: Si se habilita este ajuste, se activarán las alertas en el iDRAC (si están deshabilitadas) y se establecerá un destino de alerta para la dirección IP del servidor OpenManage Enterprise. Si hay alertas específicas que se deben habilitar, debe configurarlas en el iDRAC activando los filtros de alerta y las capturas SNMP correspondientes. Para obtener más información, consulte la Guía del usuario del iDRAC.

9. Seleccione **Establecer cadena de comunidad para el destino trap desde la configuración de la aplicación**. Esta opción está disponible solamente para los servidores iDRAC y chasis MX7000 detectados.
10. Seleccione la casilla de verificación **Enviar por correo electrónico cuando esté terminado** y, a continuación, escriba la dirección de correo electrónico en la cual desea recibir las notificaciones sobre el estado de los trabajos de detección. Si no se configura el correo electrónico, se muestra el vínculo **Ir a la configuración de SMTP**. Haga clic en el vínculo y configure los ajustes de SMTP. Consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122. Si selecciona esta opción, pero no se configura SMTP, no se muestra el botón **Finalizar** para continuar con la tarea.
11. Haga clic en **Finish** (Finalizar). No se muestra el botón Finalizar si los campos son incorrectos o están incompletos.
    Se crea y ejecuta un trabajo de detección. El estado se muestra en la página **Detalle del trabajo**.

Durante la detección de los dispositivos, la cuenta de usuario que se especifica para el rango de detección se comprueba con respecto a todos los privilegios disponibles activados en un dispositivo remoto. Si la autenticación de usuario se aprueba, el dispositivo automáticamente se incorpora o se puede incorporar posteriormente con diferentes credenciales de usuario. Consulte Incorporación de dispositivos en la página 44.

NOTA: Durante la detección de CMC, los servidores y los módulos de IOM y de almacenamiento (configurado con la dirección IP y el SNMP configurado para "público" como cadena de comunidad), que residen en el CMC también se detectaron e incorporaron. Si activa la recepción de captura durante la detección de CMC, OpenManage Enterprise se establece como el destino de captura en todos los servidores y no en el chasis.

NOTA: Durante la detección de CMC, no se detectan agregadores de I/O de FN en modo MUX programable (PMUX).

Incorporación de dispositivos

La integración permite que se administren los servidores, en lugar de que simplemente se supervisen.

- Si se proporcionan credenciales de nivel de administrador durante la detección, los servidores se incorporan (se muestra el estado del dispositivo como "administrado" en la vista Todos los dispositivos).
- Si se proporcionan credenciales con menos privilegios durante la detección, los servidores no se incorporan (el estado se muestra como "supervisado" en la vista Todos los dispositivos).
- Si la consola también está configurada como receptor de capturas en los servidores, entonces se indica el estado de incorporación como "administrado con alertas".
- **Error**: indica un problema en la integración del dispositivo.
- **Proxy**: disponible solo para chasis MX7000. Indica que el dispositivo se detecta a través de un chasis MX7000 y no directamente.

Si desea incorporar dispositivos con una cuenta de usuario diferente de la cuenta especificada para detección o volver a intentar la incorporación debido a una falla en la incorporación durante la detección, realice las siguientes tareas:

NOTA:

- Todos los dispositivos que se han incorporado a través de este asistente permanecen incorporados a través de esta cuenta de usuario y la cuenta de usuario de detección no los sustituye durante detecciones futuras de estos dispositivos.
- En el caso de los dispositivos ya detectados, si el destino trap de SNMP se establece “manualmente” en iDRAC como OpenManage Enterprise, el dispositivo recibe y procesa las alertas. Sin embargo, el estado administrado del dispositivo que se muestra en la página Todos los dispositivos sigue siendo el mismo que su estado descubierto inicial de “Monitoreado” o “Administrado con alertas”.
- En la página Todos los dispositivos, se muestra el **Estado administrado** de todo los chasis incorporados como "administrado", independientemente de las credenciales de función del usuario del chasis que se utilizaron en el momento de la incorporación. Si el chasis se incorporó con las credenciales de un usuario de "solo lectura", es posible que se produzca una falla durante las actividades de actualización realizadas en el chasis. Por lo tanto, se recomienda incorporar un chasis con las credenciales de un administrador de chasis para poder realizar todas las actividades.

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. En el menú **OpenManage Enterprise**, en **Dispositivos**, haga clic en **Todos los dispositivos**.
   Un gráfico de anillos indica el estado de todos los dispositivos en el panel de trabajo. Consulte el Gráfico de anillo. La tabla muestra las propiedades de los dispositivos seleccionados junto con su estado siguiente de incorporación:
   - **Error**: el dispositivo no se puede incorporar. Intente iniciar sesión con los privilegios recomendados. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
   - **Administrado**: el dispositivo se incorporó correctamente y se puede administrar mediante la consola de OpenManage Enterprise.
   - **Supervisado**: el dispositivo no tiene opción de administración (como la que se detectó mediante SNMP).
   - **Administrado con alertas**: el dispositivo se incorporó correctamente y la consola de OpenManage Enterprise registró correctamente su dirección IP con el dispositivo como destino trap durante la detección.
2. En el panel de trabajo, seleccione la casilla de verificación correspondiente a los dispositivos y haga clic en **Más acciones** > **Incorporación**.
   Asegúrese de seleccionar solamente los tipos de dispositivo en la página Todos los dispositivos que se admiten para la incorporación. Puede buscar dispositivos adecuados en la tabla si hace clic en **Filtros avanzados** y selecciona o escribe datos de estado de incorporación en la casilla de filtro.
   NOTA: Todos los dispositivos que se detectan no se admiten para la incorporación y solo iDRAC y CMC son compatibles. Asegúrese de seleccionar la opción de incorporación para el tipo de dispositivo compatible.
3. En el cuadro de diálogo **Incorporación**, escriba las credenciales de WS-Man: nombre de usuario y contraseña.
4. En la sección **Configuración de conexión**:
   a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
   b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
      NOTA: Si el valor de tiempo de espera ingresado es mayor que el tiempo actual de expiración de sesión, se cerrará la sesión de OpenManage Enterprise de forma automática. Sin embargo, si el valor está dentro de la ventana actual de tiempo de expiración de sesión, la sesión se mantiene y no se cierra.
   c. En la casilla **Puerto**, ingrese el número de puerto que debe utilizar el trabajo para lograr la detección.
   d. Campo opcional. Seleccione **Activar verificación de nombre común (CN)**.
   e. Campo opcional. Seleccione **Habilitar comprobación de entidad de certificación (CA)** y busque el archivo de certificado.
5. Haga clic en **Finalizar**.
   NOTA: La casilla de verificación **Habilitar recepción de captura de servidores detectados** solo es eficaz para servidores detectados por medio de la interfaz de iDRAC. La selección no es eficiente en otros servidores: como aquellos dispositivos detectados por la detección del OS.

Matriz de soporte de protocolos para detectar dispositivos

La siguiente tabla proporciona información sobre los protocolos compatibles con la detección de dispositivos.

NOTA: La funcionalidad de los protocolos compatibles para detectar, supervisar y administrar los servidores PowerEdge YX1X con iDRAC6 es limitada. Consulte Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

Tabla 13. Matriz de compatibilidad de protocolos para detección

Dispositivo/ sistema operativo	Protocolos						
	Administración de servicios web (WS-Man)	**Redfish**	**Protocolo simple de administración de red (SNMP)**	**Shell seguro (SSH)**	**Interfaz de administración de plataforma inteligente (IPMI)**	**ESXi (VMWare)**	**HTTPS**
iDRAC6 o posteriores	**Compatible**	**Compatible** Solo para iDRAC9	No compatible	No compatible	No compatible	No compatible	No compatible

Tabla 13. Matriz de compatibilidad de protocolos para detección (continuación)

Dispositivo/ sistema operativo	Protocolos						
	Administración de servicios web (WS-Man)	Redfish	Protocolo simple de administración de red (SNMP)	Shell seguro (SSH)	Interfaz de administración de plataforma inteligente (IPMI)	ESXi (VMWare)	HTTPS
		versión 4.40.10.00 y versiones posteriores **No compatible**					
PowerEdge C *	**Compatible**	No compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Chasis PowerEdge (CMC)	**Compatible**	No compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Chasis PowerEdge MX7000	No compatible	**Compatible**	No compatible	No compatible	No compatible	No compatible	No compatible
Dispositivos de almacenamiento	No compatible	No compatible	**Compatible**	No compatible	No compatible	No compatible	No compatible
Switch Ethernet	No compatible	No compatible	**Compatible**	No compatible	No compatible	No compatible	No compatible
ESXi	No compatible	No compatible	No compatible	No compatible	No compatible	**Compatible**	No compatible
Linux	No compatible	No compatible	No compatible	**Compatible**	No compatible	No compatible	No compatible
Windows	No compatible	No compatible	No compatible	**Compatible**	No compatible	No compatible	No compatible
Hyper-V	No compatible	No compatible	No compatible	**Compatible**	No compatible	No compatible	No compatible
Servidores que no son Dell	No compatible	No compatible	No compatible	No compatible	**Compatible**	No compatible	No compatible
PowerVault ME	No compatible	No compatible	No compatible	No compatible	**Compatible**	No compatible	**Compatible**

Visualizar los detalles del trabajo de detección de dispositivos

1. Haga clic en **Monitorear** > **Detección**.
2. Seleccione la fila correspondiente al nombre del trabajo de detección y, a continuación, haga clic en **Ver detalles** en el panel derecho. En la página **Detalles del trabajo** se puede encontrar la información respectiva del trabajo de detección.
3. Para obtener más información acerca de la administración de trabajos, consulte Utilización de trabajos para el control de dispositivos en la página 128.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Editar un trabajo de detección de dispositivos

Puede editar solo un trabajo de detección de dispositivos a la vez.

1. Seleccione la casilla de verificación correspondiente al trabajo de detección que desee editar y haga clic en **Editar**.
2. En el cuadro de diálogo **Crear trabajo de detección**, edite las propiedades.
   Para obtener más información sobre las tareas que se realizan en este cuadro de diálogo, consulte Creación de un trabajo de detección de dispositivos.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Ejecutar un trabajo de detección de dispositivos

NOTA: No se puede volver a ejecutar un trabajo que ya está en ejecución.

Para ejecutar trabajos de detección de dispositivos:

1. En la lista de trabajos de detección de dispositivos existentes, seleccione la casilla de verificación correspondiente al trabajo que desea ejecutar ahora.
2. Haga clic en **Ejecutar**.
   El trabajo se inicia inmediatamente y aparece el siguiente mensaje en la esquina inferior derecha.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Detener un trabajo de detección de dispositivos

Solo puede detener el trabajo si se está ejecutando. Los trabajos de detección que se hayan completado o hayan fallado no se pueden detener. Para detener un trabajo:

1. En la lista de trabajos de detección existentes, seleccione la casilla de verificación correspondiente a los trabajos que desee detener.

   NOTA: No se pueden detener varios trabajos a la vez.

2. Haga clic en **Detener**.
   De este modo, el trabajo se detiene y aparece un mensaje en la esquina inferior derecha.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Especificar varios dispositivos mediante la importación de datos desde el archivo .csv

1. En el cuadro de diálogo **Crear trabajo de detección**, de manera predeterminada, se completa un **Nombre de trabajo de detección**. Para cambiarlo, escriba un nombre de trabajo de detección.
2. Haga clic en **Importar**.

   NOTA: Descargue el archivo .CSV de muestra si es necesario.

3. En el cuadro de diálogo **Importar**, haga clic en **Importar**, busque el archivo .CSV que contiene una lista de rangos válidos y, a continuación, haga clic en **Aceptar**.

   NOTA: Aparece un mensaje de error si el archivo .CSV contiene rangos no válidos y se excluyen los rangos duplicados durante la operación de importación.

Exclusión global de rangos

Mediante el asistente para Exclusión global de rangos, puede ingresar las direcciones o el rango de dispositivos que se deben excluir de las actividades de administración y monitoreo de OpenManage Enterprise. En los siguientes pasos, se describe cómo puede excluir el rango de dispositivos:

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: En este momento, no se puede excluir un dispositivo utilizando su nombre de host, pero sí excluir solo utilizando su dirección IP o FQDN.

1. A fin de activar el asistente para Exclusión global de rangos, puede realizar una de las siguientes acciones:
   - En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), en el menú desplegable **Detección**, haga clic en **Editar rangos de exclusión**.
   - En **Monitorear** > **Detección**, haga clic en la **Lista de exclusión global** en la esquina superior derecha.
2. En el cuadro de diálogo **Exclusión global de rangos**:
   a. En el cuadro **Descripción de rango de exclusión**, escriba la información sobre el rango que se está excluyendo.
   b. En el cuadro **Ingresar rangos de exclusión**, escriba las direcciones o los rangos de los dispositivos que desee excluir. La casilla puede tomar hasta 1000 entradas de direcciones a la vez, pero separadas por un salto de línea. Es decir, cada rango de exclusiones se debe ingresar en diferentes líneas dentro del cuadro.
   El rango que se puede excluir es el mismo que los intervalos admitidos que se aplican durante la detección de un dispositivo. Consulte Crear un trabajo de detección de dispositivos en la página 43.

   NOTA:
   - El tamaño del rango se limita a 16.385 (0x4001).
   - También se admiten los formatos de CIDR IPv6 e IPv6.
3. Haga clic en **Agregar**.
4. Cuando se le solicite, haga clic en **SÍ**.
   La dirección IP o el rango se excluye de manera global y, a continuación, se muestra en la lista de rangos excluidos. Estos dispositivos se excluyen globalmente, lo que implica que no participan en actividades realizadas por OpenManage Enterprise.

   NOTA: El dispositivo que se excluye de manera global se identifica claramente como "se excluyó de manera global" en la página **Detalles del trajajo**.

   Para quitar un dispositivo de la lista de exclusión global:
   a. Seleccione la casilla de verificación y haga clic en **Quitar de exclusión**.
   b. Cuando se le solicite, haga clic en **SÍ**. El dispositivo se elimina de la lista de exclusión global. Sin embargo, OpenManage Enterprise no supervisa automáticamente los dispositivos que se quitan de la lista de exclusión global. Para que OpenManage Enterprise comience a supervisar el dispositivo, primero debe detectarlo.

NOTA:
- La adición de dispositivos que la consola ya conoce (es decir, la consola los detectó) a la lista de exclusión global no provocará la eliminación del dispositivo de OpenManage Enterprise.
- Los dispositivos incluidos recientemente en la Lista de exclusión global todavía se ven en la cuadrícula Todos los dispositivos hasta el próximo ciclo de detección. Para evitar que se realicen tareas en estos dispositivos, se recomienda que el usuario marque la casilla de verificación correspondiente a los dispositivos y, a continuación, haga clic en **Excluir** para excluirlos de forma manual de la página Todos los dispositivos.
- Los dispositivos que aparecen en la Lista de exclusión global se excluyen de todas las tareas en la consola. Si la dirección IP de un dispositivo se encuentra en la Lista de exclusión global y se crea una tarea de detección en que el rango de detección incluye esa dirección IP, ese dispositivo no será detectado. Sin embargo, no habrá indicios de error en la consola cuando se esté creando la tarea de detección. Si espera que un dispositivo se detecte y esto no ocurre, debe comprobar la Lista de exclusión global para ver si el dispositivo está incluido en ella.

.

Especificar el modo de detección para crear un trabajo de detección de servidores

1. En el menú desplegable **Tipo de dispositivo**, seleccione **SERVIDOR**.
2. Cuando se le solicite, seleccione:
   - **Dell iDRAC**: para detectar mediante iDRAC.
   - **SO del host**: para detectar mediante un sistema operativo VMware ESXi, Microsoft Windows Hyper-V o Linux.
   - **Servidores que no son Dell (vía OOB)**: para detectar servidores de terceros mediante IPMI.
3. Haga clic en **Aceptar**.
   En función de su selección, los campos se modifican en **Configuración**.
4. Escriba la dirección IP, el nombre de host o el rango IP asociado con el protocolo en **Dirección IP/Nombre de host/Rango**.
5. En **Configuración**, escriba el nombre de usuario y la contraseña del servidor que se debe detectar.
6. Para personalizar protocolos de detección haciendo clic en **Configuración adicional**, consulte Creación de plantillas personalizadas de trabajos de detección de dispositivos para servidores.
7. Programe el trabajo de detección. Consulte Definiciones de los campos Programar trabajos en la página 179.
8. Haga clic en **Finalizar**.
   Un trabajo de detección se crea y se muestra en la lista de trabajos de detección.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección

En el cuadro de diálogo **Configuración adicional**, ingrese los detalles del protocolo apropiado con el que desea detectar los servidores:

NOTA: Los protocolos apropiados se preseleccionan automáticamente en función de sus entradas iniciales.

1. Para **Detectar mediante WS-Man/Redfish (iDRAC, servidor o chasis)**
   a. En la sección Credenciales, ingrese **Nombre de usuario** y **Contraseña**.
   b. En la sección **Configuración de conexión**:
      - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
      - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
      - Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32
      - Seleccione la casilla de verificación **Activar nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
      - Seleccione la casilla de verificación **Habilitar autoridad de certificación (CA)** en caso de ser necesario.
2. Para **Detectar mediante IPMI (no Dell mediante OOB)**
   a. En la sección Credenciales, ingrese **Nombre de usuario** y **Contraseña**.
   b. En la sección **Configuración de conexión**:
      - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
      - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
      - En el cuadro **KgKey**, ingrese un valor apropiado.
3. Para **Detectar mediante SSH (Linux, Windows, Hyper-V)**

   NOTA: Solo se admite OpenSSH en Hyper-V y Windows. El protocolo SSH de Cygwin no es compatible.

   a. En la sección Credenciales, ingrese **Nombre de usuario** y **Contraseña**.
   b. En la sección **Configuración de conexión**:

- En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
- En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
- Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 22 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32
- Seleccione la casilla de verificación **Comprobar la clave del host conocido** para validar el host con respecto a las claves del host conocido.

  NOTA: Las claves del host conocido se agregan a través del servicio */DeviceService/HostKeys REST API*. Consulte la guía de la *Guía de API RESTful de OpenManage Enterprise* para obtener más información sobre cómo administrar las claves de host.
- Seleccione la casilla de verificación **Utilizar opción SUDO** si se prefiere usar cuentas SUDO.

  NOTA: Para que las cuentas SUDO funcionen, el archivo `/etc/sudoer` de los servidores se debe configurar para que se pueda utilizar NOPASSWD.

4. Para **Detectar mediante ESXi (VMware)**
   a. En la sección Credenciales, ingrese **Nombre de usuario** y **Contraseña**.
   b. En la sección **Configuración de conexión**:
      - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
      - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
      - Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32
      - Seleccione la casilla de verificación **Activar nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
      - Seleccione la casilla de verificación **Habilitar autoridad de certificación (CA)** en caso de ser necesario.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Especificar el modo de detección para crear un trabajo de detección de chasis

1. En el menú desplegable **Tipo de dispositivo**, seleccione **CHASIS**.
   En función de su selección, los campos se modifican en **Configuración**.
2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
3. En **Configuración**, escriba el nombre de usuario y la contraseña del servidor que se debe detectar.
4. Escriba el tipo de comunidad.
5. Para crear plantillas de detección personalizadas cuando se hace clic en **Configuración adicional**, consulte Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección en la página 51.

NOTA: En la actualidad, en todos los chasis M1000e detectados, la fecha en la columna FECHA Y HORA en Registros de hardware es 12 de ENE de 2013 en CMC 5.1x y versiones anteriores. Sin embargo, en todas las versiones de chasis CMC VRTX y FX2, aparece la fecha correcta.

NOTA: Cuando se detecta por separado un servidor en un chasis, la información de ranura acerca del servidor no se muestra en la sección **Información del chasis**. Sin embargo, cuando se detecta mediante un chasis, sí se muestra la información de ranura. Por ejemplo, un servidor MX740c en un chasis MX7000.

Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección

En el cuadro de diálogo **Credenciales adicionales**:

1. Seleccione **Detectar usando WS-Man/Redfish (iDRAC, servidor o chasis)**.

   NOTA: Para el chasis, la casilla de verificación **Detectar mediante WS-Man/Redfish** está seleccionada de forma predeterminada. Implica que el chasis se puede detectar utilizando cualquiera de estos dos protocolos. Los chasis M1000e, CMC VRTX y FX2 admiten los comandos de WS-Man. El chasis MX7000 admite el protocolo Redfish.

2. Ingrese el nombre de usuario y la contraseña del chasis que desea detectar.
3. En la sección **Configuración de conexión**:
   a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
   b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
   c. Escriba en la casilla **Puerto** para editar el número de puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos, consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
   d. Seleccione la casilla de verificación **Activar verificación de nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
   e. Seleccione la casilla de verificación **Habilitar comprobación de entidad de certificación (CA)**.
4. Para detectar los módulos de E/S, seleccione la casilla de verificación**Detectar los módulos de E/S con el chasis**.

   NOTA: Solo se aplica a los chasis CMC VRTX, M1000e y FX2 (modelos FN2210S, FN410T y FN410S). En el caso del chasis MX7000, los módulos de E/S se detectan automáticamente.

   NOTA: Solo los módulos de E/S con modos independientes, PMUX (MUX programable), VLT (Enlace troncal virtual) son visibles. Los modos de conmutador completo o apilados no se detectarán.

   a. Seleccione **Usar credenciales del chasis** si las credenciales de usuario del agregador M de E/S son las mismas que las del chasis.
   b. Seleccione **Usar credenciales diferentes** si las credenciales de usuario del agregador M de E/S son diferentes de las credenciales del chasis y realice los siguientes pasos:
      - Ingrese el **Nombre de usuario** y la **Contraseña**.
      - Cambie los valores predeterminados para **Reintentos**, **Tiempo de espera** y **Puerto** si es necesario.
      - Seleccione **Comprobar la clave del host conocido** para validar el host con respecto a las claves del host conocido.

        NOTA: Las claves del host conocido se agregan a través del servicio */DeviceService/HostKeys REST API*. Consulte la guía de la *Guía de API RESTful de OpenManage Enterprise* para obtener más información sobre cómo administrar las claves de host.
      - Seleccione **Utilizar opción SUDO** si es necesario.
5. Haga clic en **Finalizar**.
6. Realice las tareas en Crear un trabajo de detección de dispositivos en la página 43.

Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell

1. En el menú desplegable **Tipo de dispositivo**, seleccione **DELL STORAGE**.
2. Cuando se le solicite, seleccione:
   - PowerVault ME: para detectar los dispositivos de almacenamiento utilizando el protocolo HTTPS como PowerVault ME.
   - Otros: para detectar dispositivos de almacenamiento que utilizan protocolo SNMP.

   En función de su selección, los campos se modifican en **Configuración**.
3. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
4. En **Configuración**, según su selección inicial: ingrese el **Nombre de usuario** y la **Contraseña** para el almacenamiento HTTPS o ingrese la **Versión de SNMP** y el **tipo de comunidad** del dispositivo que se debe detectar.

5. Haga clic en **Ajustes adicionales** para personalizar el protocolo de detección correspondiente. Consulte Creación de plantillas personalizadas de trabajos de detección de dispositivos para dispositivos SNMP o consulte Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPPS: configuración adicional para los protocolos de detección en la página 52.
6. Realice las tareas en Crear un trabajo de detección de dispositivos en la página 43.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Especificar el modo de detección para crear un trabajo de detección de conmutadores de red

1. En el menú desplegable **Tipo de dispositivo**, seleccione **CONMUTADOR DE RED**.
2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
3. En **Configuración**, ingrese la **Versión de SNMP** y el **tipo de comunidad** del dispositivo que se debe detectar.
4. Haga clic en **Ajustes adicionales** para personalizar el protocolo de detección correspondiente. Consulte Creación de plantillas personalizadas de trabajos de detección de dispositivos para dispositivos SNMP
5. Realice las tareas en Crear un trabajo de detección de dispositivos en la página 43.

Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPPS: configuración adicional para los protocolos de detección

En el cuadro de diálogo **Credenciales adicionales**:

1. Ingrese el nombre de usuario y la contraseña de PowerVault ME que se detectarán.
2. En la sección **Configuración de conexión**:
   a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
   b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
   c. Escriba en la casilla **Puerto** para editar el número de puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos, consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
   d. Seleccione la casilla de verificación **Activar verificación de nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
   e. Seleccione la casilla de verificación **Habilitar comprobación de entidad de certificación (CA)**.
3. Haga clic en **Finalizar**.
4. Realice las tareas en Crear un trabajo de detección de dispositivos en la página 43.

Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP

De manera predeterminada, la casilla de verificación **Detectar con SNMP** está seleccionada para permitir la detección de almacenamiento, sistema de red u otros dispositivos SNMP.

NOTA: Solo los módulos de E/S con modos independientes, PMUX (MUX programable), VLT (Enlace troncal virtual) son visibles. Los modos de conmutador completo o apilados no se detectarán.

1. En **Credenciales**, seleccione la versión de SNMP y, a continuación, ingrese el tipo de comunidad.
2. En la sección **Configuración de conexión**:

a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
c. En la casilla **Puerto**, ingrese el número de puerto que debe utilizar el trabajo para lograr la detección.

NOTA: Actualmente, la configuración de la **casilla Reintentos** y la **casilla Tiempo de espera agotado** no tiene ningún efecto funcional en los trabajos de detección de los dispositivos de SNMP. Por lo tanto, esta configuración se puede omitir.

3. Haga clic en **Finalizar**.
4. Realice las tareas en Crear un trabajo de detección de dispositivos en la página 43.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Especificar el modo de detección para crear VARIOS trabajos de detección

1. En el menú desplegable **Tipo**, seleccione **VARIOS** para detectar dispositivos mediante varios protocolos.
2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
3. Para crear plantillas de detección personalizadas cuando se hace clic en **Configuración adicional**, consulte Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección en la página 49.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

Eliminar un trabajo de detección de dispositivos

NOTA: Se puede eliminar un dispositivo incluso cuando se están ejecutando tareas en él. La tarea que se inicia en un dispositivo falla si se elimina el dispositivo antes de la conclusión.

Para eliminar de un trabajo de detección de dispositivos:

1. Seleccione la casilla de verificación correspondiente al trabajo de detección que desee eliminar y luego haga clic en **Eliminar**.
2. Cuando se le pregunte si se pueden eliminar los trabajos, haga clic en **SÍ**.
   Los trabajos de detección se eliminan y aparece un mensaje en la esquina inferior derecha de la pantalla.

NOTA: Si elimina un trabajo de detección, los dispositivos relacionados con el trabajo no se eliminan. Si desea eliminar de la consola aquellos dispositivos detectados por una tarea de detección, elimínelos en la página **Todos los dispositivos**.

NOTA: No se puede eliminar un trabajo de detección de dispositivos de la página **Trabajos**.

Información relacionada

Detección de dispositivos para la supervisión o administración en la página 40

8

Administrar dispositivos y grupos de dispositivos

Cuando haga clic en **OpenManage Enterprise** > **Dispositivos**, podrá ver y administrar los dispositivos y los grupos de dispositivos detectados en OpenManage Enterprise. Si inició sesión como administrador de dispositivos, solo podrá ver y administrar los grupos de dispositivos y árboles asociados que se encuentran dentro de su alcance.

En el panel izquierdo, se muestran los grupos de dispositivos de la siguiente manera:

- Todos los dispositivos: El grupo raíz de nivel superior que contiene todos los grupos.
- Grupos de sistema: Grupos predeterminados creados en OpenManage Enterprise de forma predeterminada.
- Grupos personalizados: Grupos que crean los usuarios, como administradores y administradores de dispositivos. Puede crear grupos de "consulta" o "estáticos" en grupos personalizados.
- Grupos de plug-ins: Grupos creados mediante plug-ins.

Puede crear grupos secundarios en estos grupos principales. Para obtener más información, consulte Grupos de dispositivos.

En la parte superior del panel de trabajo, los gráficos de anillos muestran la condición y las alertas de todos los dispositivos de forma predeterminada. Sin embargo, cuando se seleccione un grupo en el panel izquierdo, estos gráficos de anillos mostrarán la condición y las alertas del grupo seleccionado. Además, si se instala un plug-in, es posible que se incluya un tercer gráfico de anillos que muestre los datos del plug-in instalado. Para obtener más información sobre el gráfico de anillo, consulte Gráfico de anillo.

En la tabla que figura después del gráfico de anillos, se enumeran los dispositivos y se muestra la condición, el estado de alimentación, el nombre, la dirección IP y el identificador de cada uno. De forma predeterminada, se muestran todos los dispositivos; sin embargo, cuando se selecciona un grupo en el panel izquierdo, solo se muestran los dispositivos de ese grupo. Para obtener más información sobre la lista de dispositivos, consulte Lista de dispositivos.

Los **Filtros avanzados** se pueden utilizar para limitar aún más los dispositivos que se muestran en Lista de dispositivos en función de su condición, el estado de alimentación, el estado de la conexión, el nombre, la dirección IP, el identificador, el tipo de dispositivo, el estado administrado, etc.

Cuando se selecciona un dispositivo en la lista, en el panel derecho se muestra la vista previa del dispositivo seleccionado. Cuando se seleccionan varios dispositivos, se muestra la vista previa sobre el último dispositivo seleccionado. En **Acciones rápidas**, se indican los vínculos de administración que se relacionan con el dispositivo correspondiente. Para borrar las selecciones, haga clic en **Borrar selección**.

NOTA:

- Después de actualizar OpenManage Enterprise a la versión más reciente, la lista de dispositivos se actualizará después de volver a ejecutar los trabajos de detección.
- Puede seleccionar un máximo de 25 dispositivos por página y navegar por las páginas para seleccionar más dispositivos y realizar tareas.
- Algunas de las tareas relacionadas con los dispositivos que puede realizar en la página Todos los dispositivos, como actualización de firmware, actualización de inventario, actualización de estado y acciones de control del servidor, también se pueden realizar en las páginas **Detalles de dispositivo** de dispositivos individuales.

Temas:

Organizar los dispositivos en grupos

Para una administración efectiva y rápida de los dispositivos, en un centro de datos puede:

- Agrupar los dispositivos. Por ejemplo, puede agrupar los dispositivos según las funciones, los SO, los perfiles de usuario, la ubicación, los trabajos que se ejecutan en ellos y ejecutar consultas para administrar los dispositivos.
- Filtrar los datos relacionados con el dispositivo mientras se administran los dispositivos, se actualiza el firmware, se detectan dispositivos y se administran las políticas de alertas y los informes.
- Puede administrar las propiedades de un dispositivo en un grupo. Consulte Ver y configurar dispositivos individuales en la página 67.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos supervisados por OpenManage Enterprise. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes** > **Informe de la visión general de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Para ver los datos del Panel que pertenezcan a los dispositivos o grupos seleccionados, seleccione en el menú desplegable **Grupos de dispositivos**.

NOTA: El estado de la condición de un dispositivo o grupo se indica mediante símbolos apropiados. El estado de condición de un grupo es la condición de un dispositivo en ese grupo que tiene el estado de condición más crítico. Por ejemplo, con varios dispositivos en un grupo, si la condición de un servidor es Aviso, entonces la condición del grupo también es "Aviso". El estado de resumen es igual al estado del dispositivo que tiene alta gravedad. Para obtener más información sobre el estado de resumen, consulte la documentación técnica *ADMINISTRACIÓN DEL ESTADO DE RESUMEN MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.

Los grupos pueden tener un grupo principal y un grupo secundario. Un grupo no puede tener grupos principales como su propio grupo secundario. De manera predeterminada, OpenManage Enterprise se suministra con los siguientes grupos integrados.

Grupos de sistema: grupos predeterminados que crea OpenManage Enterprise. No puede editar ni eliminar un grupo de sistemas, pero puede ver dichos grupos según los privilegios de usuario. Ejemplos de grupos de sistemas:

- **Dispositivos HCI**: dispositivos hiperconvergentes como, por ejemplo, VxRAIL y dispositivos de la serie XC de Dell EMC
- **Sistemas Hypervisor**: servidores Hyper-V y servidores VMware ESXi
- **Sistemas modulares**: chasis PowerEdge, PowerEdge FX2, chasis PowerEdge 1000e, chasis PowerEdge MX7000 y chasis PowerEdge VRTX.

  NOTA: Un chasis MX7000 puede ser un chasis principal, independiente o miembro. Si un chasis MX7000 es un chasis principal y tiene un chasis miembro, el último se detecta utilizando la IP de su chasis principal. Un chasis MX7000 se identifica mediante una de las siguientes sintaxis:

  - **Grupo de MCM**: indica el grupo de administración de varios chasis (MCM) que tiene más de un chasis identificado mediante la sintaxis siguiente: `Group_<MCM group name>_<Lead_Chassis_Svctag>` donde:
    - `<MCM group name>`: nombre del grupo de MCM
    - `<Lead_Chassis_Svctag>`: la etiqueta de servicio del chasis principal. El chasis, los sleds y los módulos de E/S de la red forman este grupo.
  - **Grupo de chasis independiente**: se identifica usando la sintaxis `<Chassis_Svctag>`. El chasis, los sleds y los módulos de E/S de la red forman este grupo.
- **Dispositivos de red**: conmutadores del sistema de red Dell Force10 y los conmutadores del Fibre Channel
- **Servidores**: servidores Dell iDRAC, servidores Linux, servidores que no son Dell, servidores de OEM y servidores Windows
- **Dispositivos de almacenamiento**: arreglos de almacenamiento Dell Compellent, arreglos de almacenamiento PowerVault MD y arreglos de almacenamiento PowerVault ME
- **Grupos de detección**: grupos que se asignan al intervalo de una tarea de detección. No se puede editar ni eliminar porque el grupo está bajo el control del trabajo de detección donde se aplica la condición incluir/excluir. Consulte Detección de dispositivos para la supervisión o administración en la página 40.

NOTA: Para expandir todos los subgrupos en un grupo, haga clic con el botón derecho del mouse en el grupo y, a continuación, haga clic en **Expandir todos**.

Grupos personalizados: Grupos que crea el administrador para requisitos específicos. Por ejemplo, se agrupan los servidores que alojan los servicios de correo electrónico. Los usuarios pueden ver, editar y eliminar según los privilegios de usuario y los tipos de grupos.

- **Grupos estáticos**: creados manualmente por el usuario cuando agrega dispositivos específicos a un grupo. Estos grupos solo cambian cuando un usuario cambia manualmente los dispositivos en el grupo o en un subgrupo. Los elementos en el grupo permanecen estáticos hasta que se edite el grupo principal o se elimine el dispositivo secundario.
- **Grupo de consulta**: grupos que se definen dinámicamente según la coincidencia con los criterios especificados por el usuario. Los dispositivos en el grupo cambian según el resultado de los dispositivos que se detectan mediante el uso de criterios. Por ejemplo, se

ejecuta una consulta para detectar servidores que están asignados al departamento de Finanzas. Sin embargo, los Grupos de consultas tienen una estructura plana sin ninguna jerarquía.

NOTA: Grupos estáticos y de consultas:

- No pueden tener más de un grupo principal. Es decir, no se puede agregar un grupo como subgrupo en su grupo principal.
- Cuando se implementan cambios en un grupo estático (se agregan o eliminan dispositivos) o en un grupo de consulta (cuando se actualiza una consulta), el cumplimiento del firmware o los controladores de los dispositivos asociados con estos grupos no se actualiza automáticamente. Se recomienda que el usuario inicie un cumplimiento de firmware o controladores para los dispositivos agregados o eliminados recientemente en dichas instancias.

NOTA: La creación de más grupos personalizados (de consultas) en la jerarquía del grupo de dispositivos impacta en el rendimiento general de OpenManage Enterprise. Para obtener un rendimiento óptimo, OpenManage Enterprise captura el estado de resumen cada 10 segundos. Tener mayor cantidad de grupos dinámicos afecta este rendimiento.

En la página **Todos los dispositivos**, en el panel izquierdo, puede crear grupos secundarios en el grupo principal estático y de consultas. Consulte Crear un grupo de dispositivos estático en la página 56 y Crear un grupo de dispositivos de consulta en la página 57.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Para eliminar el grupo secundario de un grupo estático o de consultas:

1. Haga clic con el botón derecho del mouse en grupo estático o de consultas y, a continuación, haga clic en **Eliminar**.
2. Cuando se le solicite, haga clic en **SÍ**. Se elimina el grupo y se actualiza la lista debajo del grupo.

Grupos de plug-ins: Los grupos de plug-ins se crean cuando se instalan plug-ins como Support Assist Enterprise o Power Manager Plugin. Los plug-ins, cuando están instalados, tienen sus propios grupos de sistemas y algunos, como el plug-in Power Manager, permiten que los usuarios creen grupos personalizados.

Tareas relacionadas

Eliminar dispositivos de OpenManage Enterprise en la página 62
Actualizar el inventario de dispositivos de un único dispositivo en la página 71
Actualizar la condición del dispositivo de un grupo de dispositivos en la página 64

Crear un grupo personalizado (estático o de consulta)

En **OpenManage Enterprise** > **Dispositivos** (página Todos los dispositivos), puede crear grupos estáticos o de consulta mediante el asistente para Crear grupo personalizado.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

1. A fin de activar el asistente para Crear grupo personalizado, puede hacer lo siguiente:
   - En el panel izquierdo de **OpenManage Enterprise** > **Dispositivos** GRUPOS PERSONALIZADOS, haga clic con el botón secundario en el menú vertical de tres puntos y seleccione **Crear grupo personalizado.**
   - En la página Todos los dispositivos, en el menú desplegable **Acciones de grupo**, haga clic en **Crear grupo personalizado**.
2. En el asistente para Crear grupo personalizado, seleccione uno de los siguientes grupos personalizados:
   a. **Grupo estático**
   b. **Grupo de consulta**
3. Haga clic en **Crear**.
   Según su selección (estática o de consulta), se activa el asistente para Crear grupo estático o Crear grupo de consulta.

Una vez que se crea un grupo (estático o de consulta), aparece en GRUPO PERSONALIZADO junto a los grupos estáticos o de consulta.

Crear un grupo de dispositivos estático

En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), puede crear grupos estáticos mediante el asistente para Crear grupo estático. Los dispositivos de un grupo estático permanecen estáticos hasta que se agregan o se eliminan los dispositivos del grupo.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. A fin de activar el asistente para Crear grupo estático, realice una de las siguientes acciones:
   - En GRUPOS PERSONALIZADOS, **Grupos estáticos** haga clic con el botón secundario o haga en el menú de tres puntos verticales y, luego, seleccione **Crear nuevo grupo estático**.
   - Haga clic en **Acciones de grupo** > **Crear grupo personalizado** > **Grupo estático**.
2. En el cuadro de diálogo **Asistente para Crear grupo estático**, ingrese el nombre y la descripción (opcional) del grupo y, luego, seleccione un grupo principal en el que se debe crear el nuevo grupo estático.

   NOTA: Los nombres de grupos estáticos o dinámicos y los nombres relacionados con la configuración del servidor en OpenManage Enterprise deben ser únicos (no distingue entre mayúsculas ni minúsculas). Por ejemplo, *nombre1* y *Nombre1* no se pueden utilizar al mismo tiempo.

3. Haga clic en **Siguiente**.
4. En el cuadro de diálogo Selección de miembros del grupo, seleccione los dispositivos que deben incluirse en el grupo estático.
5. Haga clic en **Finish** (Finalizar).

El grupo estático ya está creado y se incluye en el grupo principal del panel de la izquierda. Los grupos secundarios aparecen en sangría desde su grupo principal.

Crear un grupo de dispositivos de consulta

Los grupos de consulta son grupos dinámicos cuyos dispositivos se definen mediante la coincidencia de algunos criterios que especifica el usuario. Los dispositivos del grupo cambian según el resultado de los dispositivos que se detectan mediante el uso de criterios de consulta. En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), puede crear grupos de consulta mediante el asistente ara Crear grupo de consulta.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. A fin de activar el asistente para Crear grupo de consulta, puede hacer lo siguiente:
   - En grupos personalizados, haga clic con el botón secundario en **Grupos de consulta**, o haga clic en el menú de tres puntos verticales junto a los grupos de consulta y, luego, seleccione **Crear nuevo grupo de consulta.**
   - Haga clic en **Acciones de grupo** > **Crear grupo personalizado** > **Grupo de consulta**.
2. En el cuadro de diálogo **Asistente para Crear grupo de consulta**, ingrese un **nombre** y una **descripción** (opcional) para el grupo.
3. Haga clic en **Siguiente**.
4. En el cuadro de diálogo **Selección de criterios de consulta**, en el menú desplegable **Seleccione la consulta existente que desea copiar**, seleccione una consulta y, a continuación, seleccione el resto de los criterios de filtro. Consulte Seleccionar los criterios de una consulta en la página 57.
5. Haga clic en **Finish** (Finalizar).
   El grupo de consulta se crea y se coloca en la sección Grupo de consulta del panel de la izquierda.

Seleccionar los criterios de una consulta

Defina filtros cuando cree criterios de consulta para:

- Generación de informes personalizados. Consulte Creación de informes en la página 141.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte Crear un grupo de dispositivos de consulta en la página 57.

Defina los criterios de consulta mediante dos opciones:

- **Seleccionar consulta existente para copiar**: de manera predeterminada, OpenManage Enterprise proporciona una lista de plantillas de consulta incorporada que puede copiar y crear sus propios criterios de consulta. Cuando se define una consulta, se puede utilizar un máximo de 6 criterios (filtros). Para agregar filtros, debe seleccionar desde el menú desplegable **Seleccionar tipo**.
- **Seleccionar tipo**: genera criterios de consulta desde cero mediante atributos que se muestran en este menú desplegable. Los elementos en el menú dependen de los dispositivos que supervisa OpenManage Enterprise. Cuando se selecciona un tipo de consulta, se muestran solo operadores adecuados como =, >, < y null según el tipo de consulta. Se recomienda este método para definir criterios de consulta durante la elaboración de informes personalizados.

NOTA: Si se evalúa una consulta con varias condiciones, el orden de evaluación es el mismo que en SQL. Para especificar un orden en particular para la evaluación de las condiciones, agregue o quite entre paréntesis cuando defina la consulta.

NOTA: Cuando se selecciona esta opción, los filtros de los criterios de una consulta existente solo se copian virtualmente para crear un nuevo criterio de consulta. Los filtros predeterminados asociados con los criterios de una consulta existente no cambian. La definición (filtros) de criterios de consulta incorporados se utiliza como punto de partida para la creación de los criterios de una consulta personalizada. Por ejemplo:

1. *Consulta1* corresponde a criterios integrados de consulta que tiene el siguiente filtro predefinido: `Task Enabled=Yes`.
2. Copie las propiedades de filtro de *consulta1*, cree *consulta2* y, a continuación, personalice los criterios de consulta agregando otro filtro: `Task Enabled=Yes` Y `(Task Type=Discovery)`.
3. Más adelante, abra *consulta1*. Sus criterios de filtro todavía permanecen como `Task Enabled=Yes`.

1. En el cuadro de diálogo **Selección de criterios de consulta**, seleccione en el menú desplegable según si desea crear criterios de consulta para grupos de consulta o para generación de informes.
2. Agregue o quite un filtro haciendo clic en el símbolo más o en el símbolo de basurero, respectivamente.
3. Haga clic en **Finalizar**.
   Se genera un criterio de consulta y se guarda en la lista de consultas existentes. Se realiza una entrada de registro de auditoría y aparece en la lista de los registros de auditoría. Consulte Monitoreo de registros de auditoría en la página 126.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo en la página 109
Editar una línea base de cumplimiento de configuración en la página 113
Eliminar una línea base de cumplimiento de configuración en la página 115

Editar un grupo estático

En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), se puede cambiar el nombre de los grupos estáticos existentes, reposicionarlos, y los dispositivos en el grupo estático se pueden agregar o eliminar mediante el asistente para Editar grupo estático.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Haga clic con el botón secundario en el grupo estático, o haga clic en los tres puntos verticales junto al grupo estático y, luego, seleccione **Editar** a fin de activar el asistente para Editar grupo estático.
2. En el asistente para Editar grupo estático, puede editar el nombre, la descripción y el grupo principal.
3. Haga clic en **Siguiente**.
4. En la pantalla Selección de miembros del grupo, puede seleccionar (o cancelar la selección de) los dispositivos que desea incluir o excluir del grupo estático.
5. Haga clic en **Finish** (Finalizar).

Se implementan los cambios realizados en el grupo estático.

Editar un grupo de consulta

En la página Todos los dispositivos (**OpenManage Enterprise** > **Todos los dispositivos**), se puede cambiar el nombre del grupo de consulta existente, reposicionarlo, y los criterios de consulta en función de los dispositivos que se incluyen en el grupo de consulta se pueden editar mediante el asistente para Editar grupo de consulta.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. En GRUPOS PERSONALIZADOS, haga clic con el botón secundario en el grupo de consulta, o haga clic en el menú de tres puntos verticales junto al grupo de consulta y, luego, seleccione **Editar**.
2. En el asistente para Editar grupo de consulta, realice cambios en el nombre y la descripción según sea necesario.
3. Haga clic en **Siguiente**.

4. En el cuadro de diálogo Selección de criterios de consulta, en el menú desplegable **Seleccionar consulta existente para copiar**, seleccione una consulta y, luego, el resto de los criterios de filtro.
5. Haga clic en **Finish** (Finalizar).

Se implementan los cambios realizados en el grupo de consulta.

Cambiar el nombre de un grupo estático o de consulta

Para cambiar el nombre de un grupo estático o de consulta en la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), haga lo siguiente:

1. En **GRUPOS PERSONALIZADOS**, haga clic con el botón secundario en un grupo estático o de consulta, o haga clic en los tres puntos junto al grupo que desea cambiar de nombre y, luego, seleccione **Cambiar nombre**. O bien, seleccione un grupo y, luego, haga clic en **Acciones de grupo** > **Cambiar nombre del grupo**.
2. En el cuadro de diálogo **Cambiar nombre del grupo**, ingrese un nuevo nombre de grupo.
3. Haga clic en **Finalizar**.
   El nombre actualizado aparece en el panel izquierdo.

Eliminar un grupo de dispositivos estático o de consulta

En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), puede eliminar un grupo estático o de consulta existente de la siguiente manera:

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Este procedimiento se aplica solo para eliminar un grupo estático o de consulta; sin embargo, los dispositivos del grupo no se eliminarán de la página Todos los dispositivos. Para eliminar dispositivos de OpenManage Enterprise, consulte Eliminar dispositivos de OpenManage Enterprise en la página 62.

1. En **GRUPOS PERSONALIZADOS**, haga clic con el botón secundario sobre el grupo estático o de consulta, o haga clic en el menú de tres puntos verticales junto al grupo y, luego, seleccione **Eliminar**. O BIEN, seleccione el grupo que desea eliminar y, a continuación, abra el menú desplegable **Acciones de grupo** y haga clic en **Eliminar grupo**.
2. Cuando se lo solicite, haga clic en **Sí**.

El grupo se elimina de GRUPOS PERSONALIZADOS.

Clonar un grupo estático o de consulta

Los grupos estáticos o de consulta existentes se pueden clonar y agregar a los GRUPOS PERSONALIZADOS.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

1. Haga clic con el botón secundario en el grupo estático o de consulta, o haga clic en el menú de tres puntos verticales junto al grupo estático o de consulta y, luego, haga clic en **Clonar**.
2. En el cuadro de diálogo **Clonar grupo**, ingrese un nombre y una descripción para el grupo. Además, para el grupo estático, seleccione un grupo principal en el que se debe crear el estático clonado.
3. Haga clic en **Finish** (Finalizar).
   El grupo clonado se crea y se coloca en el grupo principal del panel de la izquierda.

Agregar dispositivos a un grupo nuevo

Puede crear un nuevo grupo y agregarle dispositivos desde la lista de dispositivos disponible en la página Todos los dispositivos.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. En el menú **OpenManage Enterprise**, haga clic en **Dispositivos**.
   Se muestra la página Todos los dispositivos.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos y, luego, haga clic en **Acciones de grupo** > **Agregar a nuevo grupo**.
   a. En el cuadro de diálogo **Asistente para Agregar dispositivos a un nuevo grupo**, ingrese el **Nombre** y la **Descripción** (opcional), y seleccione el **Grupo principal** en el que se creará el nuevo grupo secundario. Para obtener más información sobre los grupos, consulte Grupos de dispositivos.
   b. Para agregar más dispositivos al grupo, haga clic en **Siguiente**. O también puede ir al paso 3.
3. En el cuadro de diálogo **Selección de miembros del grupo**, seleccione más dispositivos en la lista **Agregar dispositivos**.
   Después de seleccionar los dispositivos en la lengüeta **Todos los dispositivos**, los dispositivos seleccionados se enumeran en **Todos los dispositivos seleccionados**.
4. Haga clic en **Finish** (Finalizar).
   Se crea un nuevo grupo y los dispositivos se agregan al grupo seleccionado.
   NOTA: Para crear grupos o agregar dispositivos a un grupo, debe seguir la relación principal-secundario de los grupos. Consulte Grupos de dispositivos.

Agregar dispositivos a un grupo existente

Puede agregar dispositivos a un grupo existente desde la lista de dispositivos disponible en la página Todos los dispositivos.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. En el menú **OpenManage Enterprise**, haga clic en **Dispositivos**.
   Se muestra la página Todos los dispositivos.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos y, luego, haga clic en **Acciones de grupo** > **Agregar a grupo existente**.
3. En el cuadro de diálogo **Agregar dispositivos seleccionados a un grupo existente**, ingrese o seleccione los datos. Para obtener más información sobre los grupos, consulte Grupos de dispositivos.
4. Haga clic en **Finish** (Finalizar).
   Los dispositivos se agregan al grupo existente seleccionado.
   NOTA: Para crear grupos o agregar dispositivos a un grupo, debe seguir la relación principal-secundario de los grupos. Consulte Grupos de dispositivos.

Actualizar la condición del grupo

En los siguientes pasos se describe cómo actualizar la condición y el estado en línea de un grupo seleccionado.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Para los dispositivos dentro de banda detectados mediante los sistemas operativos ESXi y Linux, el estado ( ) se muestra como Desconocido ( ).

1. Para desplazarse hasta la página Todos los dispositivos; haga clic en **OpenManage Enterprise** > **Todos los dispositivos**.
2. En el panel izquierdo, seleccione el grupo en el que desea actualizar la condición.
   Después de seleccionar el grupo, la lista de dispositivos enumerará los dispositivos del grupo seleccionado.
3. Haga clic en el menú desplegable **Actualizar condición** y, luego, haga clic en **Actualizar condición del grupo**. Se muestra el asistente Condición.
4. En el asistente Condición, **Nombre de trabajo** muestra el nombre del trabajo generado en el dispositivo para la tarea de actualización de la condición. Si es necesario, puede cambiar el nombre del trabajo.
5. El menú desplegable **Seleccionar grupo** mostrará el grupo que haya seleccionado.
6. En el menú desplegable Programación, puede seleccionar una de las siguientes opciones:
   a. **Ejecutar ahora**: para ejecutar inmediatamente la actualización de la condición del grupo seleccionado.

b. **Ejecutar más tarde**: puede seleccionar que la ejecución se realice más tarde y, luego, indicar la fecha y la hora en que se ejecutará el trabajo de actualización de condición del grupo.
c. **Ejecutar según el programa**: puede seleccionar esta opción y, luego, elegir Diariamente o Semanalmente y una hora, si desea actualizar la condición del grupo diariamente o semanalmente en un momento determinado.

Se crea un trabajo para actualizar la condición y el estado en línea del grupo. Puede ver los detalles del trabajo en la página Trabajos (**OpenManage Enterprise** > **Monitorear** > **Trabajos**).

Página Todos los dispositivos: lista de dispositivos

En la lista de dispositivos se muestran las propiedades de los dispositivos, como dirección IP y etiqueta de servicio. Puede seleccionar un máximo de 25 dispositivos por página y navegar por las páginas para seleccionar más dispositivos y realizar tareas. Para obtener más información sobre las tareas que puede realizar en la página Todos los dispositivos, consulte Página Todos los dispositivos: acciones de la lista de dispositivos en la página 61.

NOTA: De manera predeterminada, en la lista de dispositivos se muestran todos los dispositivos considerados durante la elaboración del gráfico de anillo. Para ver una lista de dispositivos pertenecientes a un estado de la condición específico, haga clic en la banda de colores correspondiente en el gráfico de anillo o haga clic en el símbolo de estado de la condición. Se incluyen en la lista aquellos dispositivos que pertenecen solo a la categoría seleccionada.

- **El estado de la condición** indica el estado de funcionamiento del dispositivo. Los estados de la condición Normal, Crítico y Advertencia se identifican mediante los respectivos símbolos de colores. Consulte Estados de los dispositivos en la página 39
- **Estado de alimentación** indica si el dispositivo está encendido o apagado
- **Estado de la conexión** indica si un dispositivo está conectado o no a OpenManage Enterprise
- **Nombre** indica el nombre del dispositivo.
- **Dirección IP** indica la dirección IP de la iDRAC instalada en el dispositivo
- **Identificador** indica la etiqueta de servicio del dispositivo
- **Modelo** indica el número de modelo
- **Tipo** indica el tipo de dispositivo, servidor, chasis, almacenamiento de Dell y switch de redes
- **Nombre del chasis** indica el nombre del chasis
- **Nombre de ranura** indica el nombre de ranura de los dispositivos del chasis
- La columna **Estado administrado** indica si el dispositivo está supervisado o administrado, o si está incorporado por proxy. Consulte Detección de dispositivos para la supervisión o administración en la página 40.

Para filtrar los datos de la tabla, haga clic en **Filtros avanzados** o en el símbolo del filtro. Para exportar datos a formato de archivo HTML, CSV o PDF, haga clic en el símbolo Exportar en la esquina superior derecha.

NOTA: En la lista Dispositivos, haga clic en el nombre del dispositivo o en una dirección IP para ver los datos de configuración del dispositivo y, a continuación, editarlos. Consulte Ver y configurar dispositivos individuales en la página 67.

NOTA: En el panel de trabajo se muestra el gráfico de anillo del grupo de dispositivos seleccionados. Con el gráfico de anillo, puede ver la lista de dispositivos que pertenecen a otros estados de la condición en ese grupo. Para ver los dispositivos de otros estados de la condición, haga clic en la banda de colores correspondiente en el gráfico de anillo. De esta manera, cambian los datos de la tabla. Para obtener más información sobre la utilización del gráfico de anillo, consulte Gráfico de anillo.

Página Todos los dispositivos: acciones de la lista de dispositivos

En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), puede realizar diversas acciones de dispositivo.

Los botones de acción son contextuales para la selección de grupos desde el árbol de la izquierda y también para los dispositivos seleccionados en la cuadrícula. Por lo tanto, las acciones relacionadas con el grupo, como "Ejecutar inventario en el grupo" y "Actualizar la condición del grupo", se ejecutarán de manera predeterminada en el grupo seleccionado. Todas las acciones de dispositivos se ejecutarán de manera predeterminada en los dispositivos seleccionados. Sin embargo, algunas acciones como Detección siempre se ejecutan sin ninguna selección. Además, el tipo de acciones disponibles para el dispositivo depende del tipo de dispositivo seleccionado.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

- Desde el menú desplegable **Acciones de grupo**, puede hacer lo siguiente:
  - Crear grupos de dispositivos personalizados. Consulte Crear un grupo personalizado (estático o de consulta) en la página 56.
  - Crear grupos estáticos. Consulte Crear un grupo de dispositivos estático en la página 56.
  - Crear grupos de consulta. Consulte Crear un grupo de dispositivos de consulta en la página 57
  - Editar grupos estáticos o de consulta. Consulte Editar un grupo estático en la página 58 y Editar un grupo de consulta en la página 58.
  - Clonar grupos. Consulte Clonar un grupo estático o de consulta en la página 59.
  - Cambiar el nombre de un grupo. Consulte Cambiar el nombre de un grupo estático o de consulta en la página 59.
  - Eliminar grupos. Consulte Eliminar un grupo de dispositivos estático o de consulta en la página 59.
  - Agregar dispositivos a un grupo nuevo. Consulte Agregar dispositivos a un grupo nuevo en la página 59.
  - Agregar dispositivos a un grupo existente. Consulte Agregar dispositivos a un grupo existente en la página 60.
- Desde el menú desplegable **Detección**, puede hacer lo siguiente:
  - Detectar e incorporar dispositivos. Consulte Detección de dispositivos para la supervisión o administración en la página 40 y Incorporación de dispositivos en la página 44.
  - Excluir dispositivos. Consulte Excluir dispositivos de OpenManage Enterprise en la página 63.
  - Editar rangos de exclusión. Consulte Exclusión global de rangos en la página 48.
- Desde el menú desplegable **Inventario**, puede hacer lo siguiente:
  - Ejecutar el inventario en un grupo de dispositivos. Consulte Crear y ejecutar un trabajo de inventario.
  - Ejecutar el inventario en los dispositivos. Consulte Ejecutar el inventario en los dispositivos en la página 63.
- Desde el menú desplegable **Actualizar condición**, puede hacer lo siguiente:
  - Actualizar la condición del grupo. Consulte Actualizar la condición del grupo en la página 60.
  - Actualizar la condición de los dispositivos. Consulte Actualizar la condición de los dispositivos en la página 65.
- Desde el menú desplegable **Más acciones**, puede hacer lo siguiente:
  - Encender LED. Consulte Crear un trabajo para encender los LED del dispositivo en la página 132.
  - Apagar LED. Consulte Crear un trabajo para encender los LED del dispositivo en la página 132.
  - Encender dispositivos. Consulte Crear un trabajo para administrar dispositivos de alimentación en la página 133.
  - Apagar dispositivos. Consulte Crear un trabajo para administrar dispositivos de alimentación en la página 133.
  - Apagar dispositivos de manera ordenada. Consulte Crear un trabajo para administrar dispositivos de alimentación en la página 133.
  - Apagar y encender un sistema (arranque en frío). Consulte Crear un trabajo para administrar dispositivos de alimentación en la página 133.
  - Reiniciar el sistema (arranque en caliente). Consulte Crear un trabajo para administrar dispositivos de alimentación en la página 133.
  - Ejecutar el comando remoto CLI de IPMI en un dispositivo. Consulte Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales en la página 70.
  - Ejecutar el comando remoto CLI de RACADM en un dispositivo. Consulte Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales en la página 70.
  - Eliminar dispositivos desde OpenManage Enterprise. Consulte Eliminar dispositivos de OpenManage Enterprise en la página 62.
  - Exportar datos de todos los dispositivos. Consulte Exportar todos los datos o aquellos seleccionados en la página 66
  - Exportar datos de los dispositivos seleccionados. Consulte Exportar todos los datos o aquellos seleccionados en la página 66

Eliminar dispositivos de OpenManage Enterprise

En los siguientes pasos, se describe cómo eliminar y desvincular dispositivos descubiertos en OpenManage Enterprise.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Un dispositivo con un perfil asignado no se puede eliminar, a menos que se desasigne el perfil. Para obtener más información, consulte Anular asignación de perfiles en la página 107.
- Se puede eliminar un dispositivo incluso cuando se están ejecutando tareas en él. Las tareas que se inician en un dispositivo fallan si se elimina el dispositivo antes de su finalización.

Para eliminar los dispositivos descubiertos:

1. Para desplazarse hasta la página Todos los dispositivos; haga clic en **OpenManage Enterprise** > **Todos los dispositivos**.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos que desea eliminar.
3. Haga clic en el menú desplegable **Más acciones** y, luego, en **Eliminar dispositivos**.

4. Cuando aparezca el mensaje que indica que los dispositivos se eliminarán y desvincularán de OpenManage Enterprise, haga clic en **SÍ**.

Los dispositivos seleccionados se eliminan por completo de OpenManage Enterprise. Después de la eliminación del dispositivo, se borra toda la información de incorporación correspondiente a los dispositivos eliminados. La información de credenciales de usuarios se elimina automáticamente si no se comparte con otros dispositivos. Si OpenManage Enterprise se configuró como destino trap en el dispositivo que se elimina, debe quitar la dirección IP de la consola de OpenManage Enterprise como destino trap del dispositivo.

Información relacionada

Organizar los dispositivos en grupos en la página 54

Excluir dispositivos de OpenManage Enterprise

Los dispositivos se descubren y se agrupan en OpenManage Enterprise para un manejo eficiente de tareas repetitivas, como actualizaciones de firmware, actualizaciones de configuración, generación de inventario y monitoreo de alertas. Sin embargo, también puede excluir dispositivos de todas las actividades de descubrimiento, monitoreo y administración de OpenManage Enterprise. Los siguientes pasos describen cómo excluir los dispositivos ya descubiertos de OpenManage Enterprise.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Para desplazarse hasta la página Todos los dispositivos; haga clic en **OpenManage Enterprise** > **Todos los dispositivos**.
2. En el panel izquierdo, seleccione el grupo del sistema o el grupo personalizado cuyo dispositivo debe excluirse.
3. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos y, luego, abra el menú desplegable **Detección** y haga clic en **Excluir dispositivos**.
4. Cuando aparezca el mensaje que indica que los dispositivos se eliminarán por completo y se agregarán a la lista de exclusión global, haga clic en **SÍ**.

Los dispositivos se excluyen, se agregan a la lista de exclusión global y OpenManage Enterprise deja de supervisarlos.

NOTA: Para quitar al dispositivo de la exclusión global y hacer que OpenManage Enterprise vuelva a monitorearlo, debe eliminar el dispositivo del rango de exclusión global y, luego, volver a detectarlo.

Ejecutar el inventario en los dispositivos

En los siguientes pasos, se describe cómo iniciar la recopilación de inventario en los dispositivos detectados.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

1. Para desplazarse hasta la página Todos los dispositivos; haga clic en **OpenManage Enterprise** > **Todos los dispositivos**.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos.
3. En el menú desplegable **Inventario**, haga clic en **Ejecutar inventario en dispositivos**.

Se crea un trabajo de inventario para la recopilación de inventario en los dispositivos seleccionados. Puede ver el estado de este trabajo en la página Inventario (**OpenManage Enterprise** > **Monitor** > **Inventario**).

Actualizar el firmware y los controladores del dispositivo mediante las bases

Puede actualizar la versión del firmware o los controladores de los dispositivos en la página Todos los dispositivos o en la página Cumplimiento del firmware/controlador (consulte Actualizar el firmware o los controladores con el informe de cumplimiento de la base en la página 82). Se recomienda realizar la actualización mediante la página Todos los dispositivos cuando se actualiza el firmware y el controlador de un mismo dispositivo.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

- Las actualizaciones de controladores solo se aplican a los dispositivos asociados con las versiones de Windows de 64 bits.
- Las actualizaciones de controladores en los dispositivos no se pueden revertir.
- Si la actualización del firmware se realiza mediante la opción "**Programar para el siguiente reinicio del servidor**", entonces la comprobación de la base y el inventario se deben ejecutar manualmente después de que el paquete esté instalado en el dispositivo remoto.
- Si el dispositivo no está relacionado con ninguna línea base, no se rellena el menú desplegable **Línea base**. Para relacionar un dispositivo con una línea base, consulte Creación de la línea base de firmware.
- Si selecciona varios dispositivos, solo los dispositivos asociados con la línea base seleccionada se muestran en la tabla.

1. En la lista **Dispositivos** de la página Todos los dispositivos, seleccione los dispositivos y haga clic en **Más acciones** > **Actualizar**.

   NOTA: Cuando selecciona dispositivos, asegúrese de que estén relacionados con una o más líneas base de firmware. De lo contrario, los dispositivos no aparecerán en el informe de cumplimiento y, por lo tanto, no se pueden actualizar.

2. En el cuadro de diálogo **Actualizar dispositivo**:
   a. En la sección **Seleccionar fuente de actualización**, seleccione una de las siguientes opciones:
      - Seleccione la base en el menú desplegable **Base**. Aparecerá una lista de dispositivos relacionados con la base seleccionada. El nivel de cumplimiento de cada dispositivo se muestra en la columna "Cumplimiento". Según el nivel de cumplimiento, puede actualizar la versión del controlador o el firmware. Para obtener más información sobre la descripción del campo en esta página, consulte Visualización del informe de cumplimiento del firmware del dispositivo.
        i. Seleccione las casillas de verificación correspondientes a los dispositivos que se deben actualizar.
        ii. Haga clic en **Siguiente**.
      - También puede actualizar el firmware o los controladores mediante el paquete individual de actualización. Haga clic en **Paquete individual** y, a continuación, siga las instrucciones que aparecen en la pantalla. Haga clic en **Siguiente**.
   b. En la sección **Programa**:
   - En **Programar actualización**, haga clic en **Información adicional** para ver la información importante y seleccione una de las siguientes opciones:
     a. **Actualizar ahora**: se aplican las actualizaciones del firmware o el controlador inmediatamente.
     b. **Programar más tarde**: se utiliza para especificar una fecha y hora en que se deba actualizar la versión del firmware o el controlador. Este modo se recomienda si no desea alterar sus tareas actuales.
   - En **Opciones del servidor**, seleccione una de las siguientes opciones de reinicio:
     a. Para reiniciar el servidor inmediatamente después de la actualización del firmware o controlador, seleccione **Reiniciar el servidor inmediatamente** y, en el menú desplegable, seleccione una de las siguientes opciones:
        i. **Reinicio ordenado sin apagado forzado**
        ii. **Reinicio ordenado con apagado forzado**
        iii. **Ciclo de encendido y apagado** para un restablecimiento forzado del dispositivo.
     b. Seleccione **Programar para el siguiente reinicio del servidor** a fin de activar la actualización del firmware o el controlador cuando se produzca el siguiente reinicio del servidor. Si se selecciona esta opción, se debe ejecutar manualmente la comprobación de la base y el inventario después de que el paquete esté instalado en el dispositivo remoto.
3. Haga clic en **Finish** (Finalizar).

Se crea un trabajo de actualización de firmware o controlador y aparece en la lista de trabajos. Consulte Utilización de trabajos para el control de dispositivos en la página 128.

Actualizar la condición del dispositivo de un grupo de dispositivos

De forma predeterminada, el dispositivo actualiza automáticamente la condición de todos los dispositivos y grupos de dispositivos cada hora; sin embargo, también puede actualizar la condición de los dispositivos o grupos de dispositivos en cualquier momento. En los siguientes pasos, se describe cómo actualizar la condición y el estado en línea de los grupos de dispositivos seleccionados en la página Todos los dispositivos.

1. En el panel izquierdo, seleccione el grupo al que pertenece el dispositivo.
   Se muestran los dispositivos asociados al grupo.
2. Seleccione la casilla de verificación correspondiente a los dispositivos y, luego, haga clic en **Actualizar condición del grupo**.
   Se crea un trabajo y aparece en la lista Trabajos, y se identifica como **Nuevo** en la columna ESTADO DEL TRABAJO.

El estado de funcionamiento más reciente de los dispositivos seleccionados se recopila y se muestra en el panel y en otras secciones pertinentes de OpenManage Enterprise. Para descargar un inventario del dispositivo, consulte Exportar el inventario de un solo dispositivo en la página 66.

Información relacionada

Organizar los dispositivos en grupos en la página 54

Actualizar la condición de los dispositivos

De forma predeterminada, el dispositivo actualiza automáticamente la condición de todos los dispositivos y grupos de dispositivos cada hora; sin embargo, también puede actualizar la condición de los dispositivos o grupos de dispositivos en cualquier momento. En los siguientes pasos, se describe cómo actualizar la condición y el estado en línea de los dispositivos seleccionados en la página Todos los dispositivos.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Para los dispositivos dentro de banda detectados mediante los sistemas operativos ESXi y Linux, el estado ( ) se muestra como Desconocido ( ).

1. Para desplazarse hasta la página Todos los dispositivos; haga clic en **OpenManage Enterprise** > **Todos los dispositivos**.
2. En la lista Dispositivos, seleccione los dispositivos en los que desea actualizar la condición.
3. Haga clic en el menú desplegable **Actualizar condición** y, luego, haga clic en **Actualizar condición de los dispositivos**.

Se inicia una tarea de condición para los dispositivos seleccionados. Puede ver el estado de la tarea de condición en la página Trabajos (**OpenManage** > **Monitorear** > **Trabajos**).

Reversar la versión del firmware de un dispositivo individual

Puede revertir la versión de firmware de un dispositivo que es posterior a la versión de firmware de la línea base a la que está asociado. Esta función solo está disponible cuando se ven y configuran las propiedades de un dispositivo individual. Consulte Ver y configurar dispositivos individuales en la página 67. Puede actualizar o revertir la versión de firmware de un dispositivo individual. Puede revertir la versión de firmware de un solo dispositivo a la vez.

NOTA:

- La reversión solo se aplica para el firmware. Los controladores del dispositivo, una vez que se actualizan, no se pueden revertir a una versión anterior.
- La reversión está destinada solo a los dispositivos que se actualizan desde la consola de OME (se puede aplicar tanto a la actualización de la base como a la de un DUP único).
- Si alguno de los iDRAC instalados no tiene el estado “listo”, un trabajo de actualización de firmware puede indicar un error aunque el firmware se haya aplicado correctamente. Revise la iDRAC que no esté en el estado listo y, a continuación, pulse F1 para continuar durante el inicio del servidor.

Cualquier firmware de dispositivo actualizado mediante el uso de la interfaz gráfica de usuario del iDRAC no aparece aquí en la lista y no se puede actualizar. Para obtener información acerca de la creación de la línea base, consulte Crear una línea de base de firmware o controladores en la página 79.

1. En el panel izquierdo, seleccione el grupo y, a continuación, haga clic en el nombre del dispositivo en la lista.
2. En la página **<nombre del dispositivo>**, haga clic en **Firmware/Controladores**.
3. En el menú desplegable **Línea base**, seleccione la línea base a la que pertenece el dispositivo.
   Se indican todos los dispositivos asociados con la línea base. Para obtener más información sobre la descripción de campo en la tabla, consulte Ver el informe de cumplimiento de la base en la página 81.
4. Seleccione la casilla de verificación correspondiente al dispositivo cuya versión del firmware debe revertirse, el cual se identifica con ..
5. Haga clic en **Revertir firmware**.
6. En el cuadro de diálogo **Revertir firmware**, se muestra la siguiente información:
   - **NOMBRE DEL COMPONENTE**: componente en el dispositivo cuya versión de firmware es posterior a la versión de línea base.
   - **VERSIÓN ACTUAL**: versión actual del componente.
   - **VERSIÓN DE LA REVERSIÓN**: versión de firmware sugerida a la que se puede degradar el componente.
   - **FUENTE DE REVERSIÓN**: haga clic en **Examinar** para seleccionar la fuente desde donde se puede descargar la versión de firmware.

7. Haga clic en **Finalizar**. La versión del firmware se revierte.

   NOTA: Actualmente, la función de reversión realiza un seguimiento solo del número de versión desde la que se revirtió el firmware. La reversión no considera la versión del firmware que esté instalada usando la función de reversión (revirtiendo la versión).

Exportar el inventario de un solo dispositivo

Puede exportar los datos de inventario de un solo dispositivo a la vez solo en formato .csv.

1. En el panel izquierdo, seleccione el grupo de dispositivos. Una lista de dispositivos en el grupo se muestra en la lista de dispositivos. Un gráfico de anillo indica el estado del dispositivo en el panel de trabajo. Consulte Gráfico de anillo. En una tabla se muestran las propiedades de los dispositivos seleccionados. Consulte Lista de dispositivos.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente al dispositivo y, a continuación, haga clic en **Exportar inventario**.
3. En el cuadro de diálogo **Guardar como**, guarde en una ubicación conocida.

   NOTA: Cuando se exportan a un formato .csv, algunos de los datos mostrados en la GUI no se muestran con una cadena descriptiva.

Cómo realizar más acciones en el chasis y en los servidores

Mediante el menú desplegable **Más acciones**, puede realizar las siguientes acciones en la página Todos los dispositivos. Seleccione los dispositivos y haga clic en cualquiera de las siguientes opciones:

- **Encender el LED**: encienda el LED del dispositivo para identificar el dispositivo entre un grupo de dispositivos en un centro de datos.
- **Apagar el LED**: apague el LED del dispositivo.
- **Encendido**: encienda los dispositivos.
- **Apagado**: apague los dispositivos.
- **Apagado ordenado**: haga clic en esta opción para apagar el sistema de destino.
- **Sistema del ciclo de apagado y encendido (reinicio mediante suministro de energía)**: haga clic en esta opción para apagar y, a continuación, reinicie el sistema.
- **Restablecimiento del sistema (reinicio flexible)**: haga clic en esta opción para apagar y, a continuación, reinicie el sistema operativo apagando de manera forzada el sistema de destino.
- **Proxy**: se muestra únicamente para el chasis MX7000. Indica que se detectó el dispositivo a través de un chasis principal MX7000 en caso de administración de varios chasis (MCM).
- **CLI de IPMI**: haga clic en esta opción para ejecutar un comando de IPMI. Consulte Crear un trabajo de comando remoto para la administración de dispositivos en la página 133.
- **CLI de RACADM**: haga clic en esta opción para ejecutar un comando de RACADM. Consulte Crear un trabajo de comando remoto para la administración de dispositivos en la página 133.
- **Actualizar firmware**: consulte Actualizar el firmware y los controladores del dispositivo mediante las bases en la página 63.
- **Incorporación**: consulte Incorporación de dispositivos en la página 44.
- **Exportar todo y seleccionados exportados**: Consulte Exportar todos los datos o aquellos seleccionados en la página 66.

Información de hardware que se muestra para el chasis MX7000

- **Suministros de energía del chasis**: información sobre las unidades de suministro de energía (PSU) que se utilizan en los sleds y otros componentes.
- **Ranuras del chasis**: información sobre las ranuras disponibles en el chasis y los componentes, si hubiera, instalados en las ranuras.
- **Controladora del chasis**: Chassis Management Controller (CMC) y su versión.
- **Ventiladores**: información acerca de los ventiladores que se utilizan en el chasis y su estado de funcionamiento.
- **Temperatura**: estado de la temperatura y los valores del umbral del chasis.
- **FRU**: componentes o unidades reemplazables en el campo (FRU) que se pueden instalar en el chasis.

Exportar todos los datos o aquellos seleccionados

Puede exportar datos:

- Sobre los dispositivos que ve en un grupo de dispositivos y realizar análisis estratégicos y estadísticos.

- Sobre un máximo de 1000 dispositivos.
- Relacionados con alertas del sistema, informes, registros de auditoría, inventario de grupos, lista de dispositivos, información sobre la garantía, SupportAssist, etc.
- En los siguientes formatos de archivo: HTML, CSV y PDF.

NOTA:
- Evite exportar tablas "amplias" que tengan columnas con cadenas largas o con demasiadas columnas a PDF. Debido a una limitación en la biblioteca de PDFMaker, la sección del extremo derecho de dichos datos exportados se trunca o se corta.
- Un inventario de dispositivo único solo se puede exportar a un formato .csv. Consulte Exportar el inventario de un solo dispositivo en la página 66
- Solo en caso de generación de informes, puede exportar únicamente los informes seleccionados a la vez y no todos los informes. Consulte Exportación de informes seleccionados en la página 142.

.

1. Para exportar datos, seleccione **Exportar todo** o **Exportar elementos seleccionados**.
   Se crea un trabajo y los datos se exportan en la ubicación seleccionada.
2. Descargue los datos y realice análisis estratégicos y estadísticos, si es necesario.
   Los datos se abren o se guardan correctamente en función de su selección.
   NOTA: Si exporta datos en formato .csv, para abrir el archivo debe contar con las credenciales de nivel de administrador.

Ver y configurar dispositivos individuales

NOTA: En la lista Dispositivos, haga clic en el nombre del dispositivo o en una dirección IP para ver los datos de configuración del dispositivo y, a continuación, edite la configuración del dispositivo como se describe en esta sección.

Haga clic en **OpenManage Enterprise** > **Dispositivos** > **Seleccionar un dispositivo de la lista de dispositivos** > **Ver detalles** para hacer lo siguiente:

- Ver la información sobre el estado y el nivel de alimentación, la IP del dispositivo y la etiqueta de servicio.
- Ver información general sobre el dispositivo y realizar tareas de solución de problemas y de control del dispositivo.
- Ver la información de dispositivos, como RAID, PSU, OS, NIC, memoria, procesador y gabinete de almacenamiento. OpenManage Enterprise ofrece un informe integrado para obtener una descripción general acerca de la NIC, el BIOS, el disco físico y el disco virtual que se utilizan en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes**.
- Actualizar o revertir las versiones de firmware de los componentes en un dispositivo que están relacionadas con una línea base de firmware. Consulte Administrar el firmware y los controladores del dispositivo en la página 75.
  NOTA: La actualización de un dispositivo mediante el flujo de trabajo de paquete individual solo es compatible con los Dell Update Packages basados en archivos ejecutables (EXE). Cuando se actualiza un CMC de FX2, el DUP ejecutable se debe instalar a través de uno de los sled en el chasis.
- Confirmar, exportar, eliminar u omitir las alertas relacionadas con un dispositivo. Consulte Administración de alertas de dispositivos.
- Ver y exportar datos de registro del hardware de un dispositivo. Consulte Administración de los registros de hardware de dispositivos individuales en la página 70.
- Ver y administrar el inventario de configuración del dispositivo para los fines de cumplimiento de la configuración. Se inicia una comparación de cumplimiento cuando el inventario de configuración se ejecuta respecto a los dispositivos.
- Ver el nivel de cumplimiento de un dispositivo comparado con la línea base de cumplimiento de la configuración con la que se encuentra asociado. Consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

Descripción general del dispositivo

- En la página **<device name>**, en **Descripción general**, se muestran el estado, el nivel de alimentación y la etiqueta de servicio del dispositivo. Haga clic en la dirección IP para abrir la página de inicio de sesión de iDRAC. Consulte la *Guía del usuario de iDRAC* disponible en el sitio de soporte de Dell.
  - **Información**: información del dispositivo, como la etiqueta de servicio, las ranuras DIMM, el nombre de DNS de iDRAC, los procesadores, el chasis, el sistema operativo y el nombre del centro de datos. Se indican varias direcciones IP de administración relacionadas con el dispositivo y se puede hacer clic en ellas para activar las interfaces correspondientes.
  - **Alertas recientes**: las últimas alertas que se generaron para el dispositivo.

- **Actividad reciente**: una lista de los trabajos recientes ejecutados en el dispositivo. Haga clic en **Ver todos** para ver todos los trabajos. Consulte Utilización de trabajos para el control de dispositivos en la página 128.
- **Consola remota**: haga clic en **Iniciar iDRAC** para iniciar la aplicación iDRAC. Haga clic en **Iniciar consola virtual** para iniciar la consola virtual. Haga clic en el símbolo **Actualizar vista previa** para actualizar la página **Vista previa**.
- **Subsistema del servidor**: muestra el estado de otros componentes del dispositivo, como la PSU, el ventilador, la CPU y la batería.

  NOTA: El tiempo necesario para recopilar datos del subsistema de los componentes del sensor descubiertos con IPMI depende de la conectividad de red, del servidor de destino y del firmware de destino. Si experimenta tiempos de espera agotados durante la recopilación de datos del sensor, reinicie el servidor de destino.
- La sección **Última actualización** indica la última vez que se actualizó el estado del inventario del dispositivo. Haga clic en el botón **Actualizar** para actualizar el estado. Se inicia un trabajo de inventario y el estado se actualiza en la página.

- Mediante el **Control de alimentación**, encienda, apague, realice el ciclo de apagado y encendido, y apague un dispositivo fácilmente.
- Mediante **Solucionar problemas**:
  - Ejecute y descargue el informe de diagnóstico. Consulte Ejecutar y descargar informes de diagnóstico en la página 69.
  - Restablezca el iDRAC.
  - Extraiga y descargue el informe de SupportAssist. Consulte Extraer y descargar informes de SupportAssist en la página 69.
- Actualice el estado del dispositivo.
- Actualice el inventario de dispositivos.
- Exporte el inventario del dispositivo que se recopila. Para ello, haga clic en **Actualizar inventario**. Consulte Exportar todos los datos o aquellos seleccionados en la página 66.
- Ejecute un comando remoto de RACADM e IPMI en el dispositivo. Consulte Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales en la página 70.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes** > **Informe de la visión general de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

Información del hardware del dispositivo

OpenManage Enterprise ofrece un informe incorporado sobre los componentes y su cumplimiento con la línea base de cumplimiento del firmware. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes** > **Cumplimiento de firmware por informe de componentes**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

- **Información de la tarjeta del dispositivo**: información sobre las tarjetas que se utilizan en el dispositivo.
- **Software instalado**: lista del firmware y el software instalados en los distintos componentes del dispositivo.
- **Procesador**: información del procesador, como zócalos, familia, velocidad, núcleos y modelo.
- **Información de la controladora RAID**: el controlador PERC y RAID que se utiliza en los dispositivos de almacenamiento. El resumen del estado es igual al estado de la RAID que tiene alta gravedad. Para obtener más información sobre el estado de Resumen de condición, consulte las notas técnicas *ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.a GENERACIÓN Y POSTERIORES* en Dell TechCenter.
- **Información de NIC**: información sobre las NIC que se utilizan en el dispositivo.
- **Información de la memoria**: los datos sobre las DIMM que se utilizan en el dispositivo.
- **Disco de matriz**: información sobre las unidades instaladas en el dispositivo. OpenManage Enterprise ofrece un informe integrado sobre los discos duros o las unidades virtuales disponibles en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes** > **Informe del disco físico**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.
- **Controladora de almacenamiento**: la controladora de almacenamiento instalada en el dispositivo. Haga clic en el símbolo más para ver los datos individuales de la controladora.
- **Información de suministro de energía**: información sobre los suministros de energía instaladas en el dispositivo.
- **Sistema operativo**: OS instalado en el dispositivo.
- **Licencias**: estado de las distintas licencias instaladas en el dispositivo.
- **Gabinete de almacenamiento**: estado del gabinete de almacenamiento y de la versión de EMM.
- **Memoria flash virtual**: lista de unidades flash virtual y sus especificaciones técnicas.
- **FRU**: lista de las Unidades reemplazables de campo (FRU, por sus siglas en inglés) que pueden gestionar y reparar únicamente los técnicos de campo. OpenManage Enterprise ofrece un informe integrado sobre las unidades reemplazables en el campo (FRU) instaladas en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise** > **Monitorear** > **Informes** > **Informe de FRU**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.
- **Información de administración de dispositivos**: información de la dirección IP de la iDRAC instalada solamente en el caso de un dispositivo de servidor.

- **Datos del huésped**: muestra los dispositivos huéspedes que OpenManage Enterprise supervisa. UUID es el identificador único universal del dispositivo. La columna **ESTADO DE LOS HUÉSPEDES** indica el estado de funcionamiento del dispositivo huésped.

Ejecutar y descargar informes de diagnóstico

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. ConsulteControl de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

1. En la página **<Device name>**, en el menú desplegable **Solucionar problemas**, seleccione **Ejecutar diagnósticos**.
2. En el cuadro de diálogo **Tipo de diagnóstico remoto**, en el menú desplegable **Tipo de diagnóstico remoto**, seleccione una de las siguientes opciones para generar un informe.
   - **Expreso**: en el menor tiempo posible.
   - **Extendido**: a la velocidad nominal.
   - **Largo plazo**: a un ritmo lento.

   NOTA: Consulte el documento técnico *Diagnóstico automatizado en ejecución remota por medio de los comandos WS-Man y RACADM* en https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.
3. Para generar el informe de diagnóstico en el momento, seleccione **Ejecutar ahora**.
4. Haga clic en **Aceptar**. Cuando se le solicite, haga clic en **SÍ**.

   AVISO: La ejecución de un informe de diagnóstico reinicia automáticamente el servidor.

   Se crea un trabajo que se muestra en la página **Trabajos**. Para ver más información sobre un trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Ver listas de trabajos en la página 128. El estado del trabajo también se muestra en la sección **Actividad reciente**. Cuando se haya ejecutado correctamente el trabajo, el estado del trabajo se indica como **Diagnóstico terminado** y el vínculo **Descargar** se muestra en la sección **Actividad reciente**.
5. Para descargar el informe, haga clic en el vínculo **Descargar** y, a continuación, descargue el archivo del informe de diagnósticos *<Servicetag-jobid>*.TXT.
   - De lo contrario, haga clic en **Solucionar problemas** > **Descargar informe de diagnóstico** y, a continuación, descargar el archivo.
6. En el cuadro de diálogo **Descargar archivos RemoteDiagnostics**, haga clic en el enlace de archivos .TXT y, a continuación, descargue el informe.
7. Haga clic en **Aceptar**.

Extraer y descargar informes de SupportAssist

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

1. En la página **<Nombre del dispositivo>**, en el menú desplegable **Solucionar problemas**, seleccione **Extraer informe de SupportAssist**.
2. En el cuadro de diálogo **Extraer informe de SupportAssist**:
   a. Ingrese el nombre del archivo donde se debe guardar el informe de SupportAssist.
   b. Seleccione las casillas de verificación correspondientes a los tipos de registro de los cuales se debe extraer un informe de SupportAssist.

3. Haga clic en **Aceptar**.
   Se crea un trabajo que se muestra en la página **Trabajos**. Para ver más información sobre un trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Ver listas de trabajos en la página 128. El estado del trabajo también se muestra en la sección **Actividad reciente**. Cuando se haya ejecutado correctamente el trabajo, el estado del trabajo se indica como **Diagnóstico terminado** y el vínculo **Descargar** se muestra en la sección **Actividad reciente**.
4. Para descargar el informe, haga clic en el vínculo **Descargar** y, a continuación, descargue el archivo del informe de SupportAssist <*Service Tag*>.<*Time*>.TXT.
   - De lo contrario, haga clic en **Solucionar problemas** > **Descargar informe de SupportAssist**.
5. En el cuadro de diálogo **Descargar archivos SupportAssist**, haga clic en el enlace de archivos .TXT y, a continuación, descargue el informe. Cada vínculo representa el tipo de registro que seleccionó.
6. Haga clic en **Aceptar**.

Administración de los registros de hardware de dispositivos individuales

NOTA: Los registros de hardware están disponibles para los servidores YX4X, chasis MX7000 y sleds. Consulte Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

- En la página **<nombre del dispositivo>**, haga clic en **Registros de hardware**. Se indican todos los sucesos y los mensajes de error generados para el dispositivo. Para obtener descripciones sobre campos, consulte Monitoreo de registros de auditoría en la página 126.
- Para un chasis, los datos en tiempo real sobre los registros de hardware se recuperan del chasis.
- Para agregar un comentario, haga clic en **Agregar comentario**.
- En el cuadro de diálogo, escriba el comentario y, a continuación, haga clic en **Guardar**. El comentario se guarda y se identifica por un símbolo en la columna **COMENTARIO**.
- Para exportar los datos de registro seleccionados a un archivo .CSV, seleccione las casillas de verificación que correspondan y, a continuación, haga clic en **Exportar** > **Exportar seleccionado**.
- Para exportar todos los registros en una página, haga clic en **Exportar** > **Exportar Página actual**.

Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales

Los comandos IPMI y RACADM se pueden enviar a la iDRAC de un dispositivo desde la página “Nombre del dispositivo” para administrar de forma remota el dispositivo correspondiente.

NOTA:

- La CLI de RACADM solo permite un comando a la vez.
- El uso de los siguientes caracteres especiales como parámetros de la CLI de IPMI y RACADM no es soportado: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * y **'**.

1. Seleccione la casilla de verificación correspondiente al dispositivo y, a continuación, haga clic en **Ver detalles**.
2. En la página <**nombre del dispositivo>**, haga clic en **Línea de comandos remota** y, a continuación, seleccione **CLI de RACADM** o **CLI de IPMI**.

   NOTA: La pestaña CLI de RACADM no aparece para los siguientes servidores, porque la tarea correspondiente no está disponible en el paquete de dispositivos: MX740c, MX840c y MX5016S.

3. En el cuadro de diálogo **Enviar comando remoto**, escriba el comando. Se puede ingresar un máximo de 100 comandos y cada comando debe estar en una línea nueva. Para mostrar los resultados en el mismo cuadro de diálogo, seleccione la casilla de verificación **Abrir los resultados después del envío**.

   NOTA: Ingrese un comando de IPMI con la siguiente sintaxis: `-I lanplus <command>` Para terminar el comando, ingrese “Exit”.

4. Haga clic en **Enviar**.
   Se crea un trabajo que se muestra en el cuadro de diálogo. El trabajo también aparece en los detalles del trabajo. Consulte Ver listas de trabajos en la página 128.
5. Haga clic en **Finalizar**.
   La sección **Alertas recientes** muestra el estado de finalización del trabajo.

Iniciar la aplicación de administración iDRAC de un dispositivo

1. Seleccione la casilla de verificación correspondiente al dispositivo.
   Aparecen el estado de funcionamiento del dispositivo, el nombre, el tipo, la dirección IP y la etiqueta de servicio.
2. En el panel derecho, haga clic en **Iniciar la aplicación de administración**.
   Aparece la página de inicio de sesión del iDRAC. Inicie sesión con el uso de las credenciales iDRAC.

   Para obtener más información sobre la utilización de iDRAC, visite Dell.com/idracmanuals.

   NOTA: También puede iniciar la aplicación de administración haciendo clic en la dirección IP en la lista de dispositivos. Consulte Página Todos los dispositivos: lista de dispositivos en la página 61.

Iniciar la consola virtual

El vínculo **Consola virtual** funciona con la licencia de iDRAC Enterprise de los servidores YX4X. En los servidores YX2X y YX3X, el vínculo funciona con las versiones 2.52.52.52 y posteriores de la licencia de iDRAC Enterprise. Haga clic en el vínculo cuando el tipo actual del complemento de la consola virtual es Active X para ver un mensaje de petición, que indica que actualice la consola para HTML 5 para mejorar la experiencia del usuario. Consulte Crear un trabajo para cambiar el tipo de complemento de la consola virtual en la página 134y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener información.

1. Seleccione la casilla de verificación correspondiente al dispositivo.
   Aparecen el estado de funcionamiento del dispositivo, el nombre, el tipo, la dirección IP y la etiqueta de servicio.
2. En el panel derecho, haga clic en **Iniciar la consola virtual**.
   Se muestra la página de la consola remota en el servidor.

Actualizar el inventario de dispositivos de un único dispositivo

De manera predeterminada, el inventario de los componentes de software y hardware en los dispositivos o grupos de dispositivos se recopila automáticamente después de cada 24 horas (por ejemplo, todos los días a las 12:00 a. m.). Sin embargo, para recolectar el informe del inventario de un único dispositivo en cualquier momento:

1. Seleccione la casilla de verificación correspondiente al dispositivo en la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**) y haga clic en **Ver detalles** en el panel derecho. Se mostrará la página Descripción general del dispositivo.
2. Haga clic en **Actualizar inventario** para iniciar un trabajo de inventario.
   El estado del trabajo de inventario se puede ver en la página Inventario (**OpenManage Enterprise** > **Monitorear** > **Inventario**). Seleccione el trabajo de inventario y haga clic en **Ver detalles** para ver el inventario recopilado del dispositivo seleccionado. Para obtener más información sobre cómo ver los datos de inventario actualizados, consulte Ver y configurar dispositivos individuales en la página 67. Para descargar un inventario del dispositivo, consulte Exportar el inventario de un solo dispositivo en la página 66.

Información relacionada

Organizar los dispositivos en grupos en la página 54

9

Administración del inventario del dispositivo

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Si hace clic en **OpenManage Enterprise** > **Supervisión** > **Inventario**, puede generar un informe del inventario de dispositivos para administrar de mejor forma el centro de datos, reducir el mantenimiento, mantener el stock al mínimo y reducir los costos operativos. Con la característica Programas de inventario en OpenManage Enterprise, puede programar trabajos para que se ejecuten en una hora predefinida y, a continuación, generar informes. Puede programar trabajos de inventario de 12.ª generación y servidores posteriores PowerEdge, dispositivos de red, chasis de PowerEdge, matrices de EqualLogic, matrices Compellent y dispositivos PowerVault.

En esta página, puede crear, editar, ejecutar, detener o eliminar programas de inventario. Se muestra una lista de trabajos de programa de inventario existentes.

- **NOMBRE**: el nombre de programación del inventario.
- **PROGRAMA**: indica si el trabajo está programado para ejecutarse ahora o más tarde.
- **ÚLTIMA EJECUCIÓN**: indica cuándo se ejecutó por última vez el trabajo.
- **ESTADO**: indica si el trabajo está en ejecución, completo o con error.

NOTA: En las páginas **Programas de detección** e **Inventario**, el estado de un trabajo programado se identifica como **En cola** en la columna **ESTADO**. Sin embargo, el mismo estado se indica como **Programado** en la página **Trabajos**.

Para obtener información de un trabajo, haga clic en la fila correspondiente al trabajo. El panel derecho muestra los datos del trabajo y los grupos de destino asociados con la tarea de inventario. Para ver información sobre el trabajo, haga clic en **Ver detalles**. La página **Detalles del trabajo** muestra más información. Consulte Visualizar la información de trabajos individuales en la página 132.

Tareas relacionadas

Ejecución de un trabajo de inventario ahora en la página 73
Detención de un trabajo de inventario en la página 73
Eliminación de un trabajo de inventario en la página 74
Creación de un trabajo de inventario en la página 72

Temas:

Creación de un trabajo de inventario

En los siguientes pasos, se describe cómo puede iniciar la recopilación de inventario en los grupos detectados.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- La recopilación de inventario en los sleds de almacenamiento del chasis no es soportada en OpenManage Enterprise si se administran a través de la administración de dispositivos del chasis.

1. A fin de iniciar el asistente para Inventario, realice una de las siguientes acciones:

a. En la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), seleccione un grupo en el panel izquierdo y, en el menú desplegable **Inventario**, haga clic en **Ejecutar el inventario en el grupo**.
b. En la página Inventario (**OpenManage Enterprise** > **Monitorear** > **Inventario**), haga clic en **Crear**.

2. En el cuadro de diálogo **Inventario**, se completa el nombre predeterminado del trabajo de inventario en **Nombre del trabajo de inventario**. Para cambiar, ingrese un nombre de trabajo de inventario.
3. En el menú desplegable **Seleccionar grupos**, seleccione los grupos de dispositivos en que se debe ejecutar el inventario.

   Si inició el trabajo de inventario desde la página Todos los dispositivos después de seleccionar un grupo, la sección Seleccionar grupos se rellena previamente con el nombre del grupo seleccionado. Para obtener información acerca de los grupos de dispositivos, consulte Organizar los dispositivos en grupos en la página 54.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior.

   Consulte Definiciones de los campos Programar trabajos en la página 179.
5. Se pueden seleccionar las siguientes **Opciones adicionales** mientras se ejecuta el trabajo de inventario:
   - Seleccione la casilla de verificación **Recolectar el inventario de la configuración** para generar un inventario de la base de cumplimiento de la configuración.
   - Seleccione la casilla de verificación **Recolectar inventario de los controladores** para recolectar información de inventario de controladores del servidor de Windows. Además, para instalar el Recolector de inventario y la Actualización del sistema Dell en el servidor de Windows si estos componentes no están disponibles en el servidor.

   NOTA:
   - "Recolectar inventario de los controladores" se aplica solo a los dispositivos detectados como servidores de Windows de 64 bits.
   - La recolección de inventario de los dispositivos basados en Windows solo se admite mediante OpenSSH. No se admiten otras implementaciones de SSH en Windows, como el protocolo SSH de CygWin.

   Para obtener información acerca de las líneas base de cumplimiento de configuración, consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.
6. Haga clic en **Finalizar**.
7. Se crea el trabajo y se muestra en la cola.
   Se crea un trabajo de inventario que se muestra en la lista de trabajos de inventario. La columna **PROGRAMA** especifica si se programó o no el trabajo. Consulte Ejecución de un trabajo de inventario ahora en la página 73.

Información relacionada

Administración del inventario del dispositivo en la página 72

Ejecución de un trabajo de inventario ahora

NOTA: No se puede volver a ejecutar un trabajo que ya está en ejecución.

1. En la lista de los trabajos de programa de inventario existentes, seleccione la casilla de verificación correspondiente al trabajo de inventario que desee ejecutar inmediatamente.
2. Haga clic en **Ejecutar ahora**.

   El trabajo se inicia inmediatamente y aparece el siguiente mensaje en la esquina inferior derecha.

Información relacionada

Administración del inventario del dispositivo en la página 72

Detención de un trabajo de inventario

Solo puede detener el trabajo si se está ejecutando. Los trabajos de inventario que se hayan completado o hayan fallado no se pueden detener. Para detener un trabajo:

1. En la lista de los trabajos de programa de inventario existentes, seleccione la casilla de verificación correspondiente al trabajo de programa de inventario que desee detener.
2. Haga clic en **Detener**.
   De este modo, el trabajo se detiene y aparece un mensaje en la esquina inferior derecha.

Información relacionada

Administración del inventario del dispositivo en la página 72

Eliminación de un trabajo de inventario

NOTA: No puede eliminar un trabajo si se está ejecutando.

1. En la lista de trabajos de programas de inventario existentes, seleccione la casilla de verificación correspondiente al trabajo de inventario que desee eliminar.
2. Haga clic en **Eliminar**.
   De este modo, el trabajo se elimina y se muestra un mensaje en la esquina inferior derecha.

Información relacionada

Administración del inventario del dispositivo en la página 72

Edición de un trabajo de programa de inventario

1. Haga clic en **Editar**.
2. En el cuadro de diálogo **Programa de inventario**, edite el nombre del trabajo de inventario en **Nombre del trabajo de inventario**.
   Consulte Creación de un trabajo de inventario en la página 72.
   La tarea del programa de inventario se actualiza y aparece en la tabla.

10

Administrar el firmware y los controladores del dispositivo

En la página **OpenManage Enterprise** > **Configuración** > **Cumplimiento del firmware/controlador**, puede administrar el firmware de todos los dispositivos "administrados". También puede actualizar los controladores de dispositivos basados en Windows de 64 bits.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Si la versión del firmware o el controlador del dispositivo es anterior a la versión de la base, no se actualiza automáticamente y el usuario debe iniciar la actualización.
- Se recomienda actualizar el firmware y los controladores durante los períodos de mantenimiento para evitar que los dispositivos o el entorno se queden offline durante el horario comercial.
- Para administrar el firmware o los controladores de un dispositivo, el estado de incorporación del sistema debe ser "Administrado" o "Administrado con alertas". Consulte Incorporación de dispositivos en la página 44
- Actualmente, el catálogo contiene controladores únicamente para los dispositivos basados en Windows de 64 bits.

Con la función Firmware/controlador, puede:

- Utilizar un catálogo de firmware y controladores de Dell.com, ya sea de forma directa o después de guardarlo en una ruta de red. ConsulteAgregar un catálogo con Dell.com en la página 76 o Creación de un catálogo de firmware mediante una red local.
- Crear una base de firmware y controladores mediante los catálogos disponibles. Estas bases sirven como referencias para comparar la versión del firmware y el controlador de los dispositivos con la versión que se encuentra en el catálogo. Consulte Creación de la línea base de firmware.
- Ejecutar un informe de cumplimiento para comprobar si los dispositivos relacionados con la base cumplen con las versiones del controlador y el firmware de la base. Consulte Comprobación de cumplimiento del firmware. La columna **CUMPLIMIENTO** muestra:
  - **Correcto** si la versión del firmware o los controladores del dispositivo objetivo es la misma que la de la base.
  - **Actualización:** si el dispositivo objetivo tiene una o varias versiones anteriores a la versión del controlador o el firmware de la línea de base. Consulte Actualización de la versión de firmware del dispositivo
  - **Crítico** Si el dispositivo no cumple con la base e indica que es una actualización crítica, y el firmware y los controladores del dispositivo deben actualizarse para garantizar un correcto funcionamiento.
  - **Advertencia** Si el firmware o los controladores del dispositivo no cumplen con la base y el firmware puede actualizarse para mejorar su funcionamiento.
  - **Cambio a una versión anterior** Si el firmware o los controladores del dispositivo son posteriores a la versión de la base.
  - Exportar el informe de cumplimiento para fines estadísticos y de análisis.
  - Actualizar la versión del firmware o los controladores del dispositivo mediante la base. Consulte Actualizar el firmware y los controladores del dispositivo mediante las bases en la página 63 .

NOTA:

- Cuando se verifica el nivel de cumplimiento de normas de una base de firmware o un controlador con muchos dispositivos, se registran alertas de advertencia CDEV9000 en la página Alertas para un solo dispositivo en incumplimiento aleatorio de esa base.
- El estado de cumplimiento del firmware o de los controladores de switches de red, IOA modulares y dispositivos Dell Storage se muestra como **Desconocido**, ya que no se puede actualizar mediante el catálogo de Dell. Se recomienda realizar actualizaciones de firmware o controlador individuales para estos dispositivos mediante su paquete de actualización individual correspondiente. Para realizar actualizaciones de firmware o controlador individuales, seleccione un dispositivo en la página Todos los dispositivos, haga clic en **Ver detalles** > **Firmware/controladores** y seleccione la opción de paquete individual. Para obtener más información sobre la lista de dispositivos no compatibles, consulte Informes de base de cumplimiento del firmware o el controlador: dispositivos con estado de cumplimiento "Desconocido" en la página 183 .

También puede actualizar la versión de firmware de un dispositivo en:

- La página Todos los dispositivos. Consulte Actualización de la versión de firmware del dispositivo.
- La página Detalles de los dispositivos. En la lista de dispositivos, haga clic en el nombre del dispositivo o en una dirección IP para ver los datos de configuración del dispositivo y, a continuación, editarlos. Consulte Ver y configurar dispositivos individuales en la página 67.

  NOTA: La actualización de un dispositivo mediante el flujo de trabajo de paquete individual solo es compatible con los Dell Update Packages basados en archivos ejecutables (EXE). Cuando se actualiza un CMC de FX2, el DUP ejecutable se debe instalar a través de uno de los sled en el chasis.

  El resumen de todas las líneas base aparece en el panel de trabajo, y el cumplimiento de una línea base seleccionada se muestra en el panel derecho mediante un gráfico de anillo. El gráfico de anillo y la lista de elementos de la base cambian en función de la base que seleccione de la lista correspondiente. Consulte Gráfico de anillo.

Temas:

Administrar catálogos de firmware y controladores

Los catálogos son paquetes de firmware y controladores basados en los tipos de dispositivos. En Dell.com se encuentran validados y publicados todos los catálogos disponibles (paquetes actualizados). Puede utilizar el catálogo directamente desde el repositorio en línea o puede descargarlo a un recurso compartido de red.

Con estos catálogos, puede crear bases de firmware o controladores para los dispositivos detectados y comprobar su nivel de cumplimiento. Esta práctica reduce el esfuerzo adicional de los administradores y los administradores de dispositivos y también reduce el tiempo general que demoran las actualizaciones y el mantenimiento.

Los usuarios administradores pueden ver todos los catálogos de OpenManage Enterprise y acceder a ellos, mientras que los administradores de dispositivos solo pueden ver y administrar los catálogos que hayan creado y les pertenezcan. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Para obtener información sobre definiciones de campos en la página Catálogo de administración, consulte Definiciones de campos de administración de catálogos en la página 183. Los orígenes de catálogo a los que puede acceder en la actualidad son los siguientes:

NOTA:
- La administración de catálogos de firmware mediante Dell.com o una ruta de red local se limita solo al catálogo de Enterprise Server.
- Los catálogos con la ubicación base que apunta a “Downloads.dell.com” se pueden utilizar sin Dell Update Packages (DUP) al importar el catálogo en OpenManage Enterprise versión 3.5 desde un recurso compartido de red. Durante el proceso de actualización del firmware, los DUP se descargarán directamente desde https://downloads.dell.com.

- **Versiones más recientes de los componentes en Dell.com**: muestra las versiones más recientes del firmware y los controladores (Windows de 64 bits) de los dispositivos. Por ejemplo, iDRAC, BIOS, PSU y unidades de disco duro que se someten a rigurosas pruebas y se liberan y publican en Dell.com. Consulte Creación de un catálogo de firmware con Dell.com.
- **Ruta de red**: corresponde a la ubicación que Dell Repository Manager (DRM) utiliza para descargar los catálogos del firmware y los controladores, y en la que tales catálogos se guardan en un recurso compartido de red. Consulte Creación de un catálogo de firmware mediante una red local.

Agregar un catálogo con Dell.com

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

1. En la página **Administración de catálogos**, haga clic en **Agregar**.

2. En el cuadro de diálogo **Agregar catálogo de actualización**:
   a. En la casilla **Nombre**, escriba un nuevo nombre del catálogo de firmware.
   b. Para la **Fuente del catálogo**, seleccione la opción **Versiones más recientes del componente de Dell.com**.
   c. En la casilla **Actualizar catálogo**, seleccione **Manual** o **Automático**.
   d. Si selecciona **Automáticamente** en el cuadro **Actualizar catálogo**, se debe definir la **Frecuencia de actualización** como **Diariamente** o **Semanalmente**, seguida de la hora en el formato de 12 horas con a. m./p. m.
   e. Haga clic en **Finalizar**.

      El botón **Terminar** aparece solo después de que ha completado todos los campos en el cuadro de diálogo

      Se crea un nuevo catálogo de firmware y se agrega en la tabla Catálogo de la página **Administración de catálogos**.
3. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

Agregar un catálogo a la red local

El catálogo que contiene el firmware y los controladores (Windows de 64 bits) se puede descargar mediante Dell Repository Manager (DRM) y guardar en un recurso compartido de red.

1. En la página **Administración de catálogos**, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar catálogo de actualización**:
   a. En la casilla **Nombre**, escriba un nuevo nombre de catálogo.
   b. Para ver la fuente del catálogo, seleccione la opción **Ruta de red**.
   Aparece el menú desplegable **Tipo de recurso compartido**.
   c. Seleccione una de las siguientes opciones:

      NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

      - NFS
        i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
        ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *nfsshare\catalog.xml*
      - CIFS
        i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
        ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *Firmware\m630sa\catalog.xml*
        iii. En la casilla **Dominio**, ingrese el nombre de dominio del dispositivo.
        iv. En la casilla **Nombre de usuario**, ingrese el nombre de usuario del dispositivo en el que se almacena el catálogo.
        v. En la casilla **Contraseña**, ingrese la contraseña del dispositivo para acceder al recurso compartido. Escriba el nombre de usuario y la contraseña de la carpeta compartida en la que está almacenado el archivo catalog.xml.
      - HTTP
        i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
        ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *compute/catalog.xml*.
      - HTTPS
        i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
        ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *compute/catalog.xml*.
        iii. En la casilla **Nombre de usuario**, ingrese el nombre de usuario del dispositivo en el que se almacena el catálogo.
        iv. En la casilla **Contraseña**, ingrese la contraseña del dispositivo en el que se almacena el catálogo.
        v. Seleccione la casilla de verificación **Comprobación de certificado**.

La autenticidad del dispositivo donde se encuentra el archivo de catálogo se valida y se genera un certificado de seguridad que aparece en el cuadro de diálogo **Información del certificado**.

d. Después de introducir la **Dirección del recurso compartido** y la **Ruta del archivo del catálogo**, aparece el vínculo **Probar ahora**. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se establece la conexión con el catálogo, aparecerá el mensaje *Conexión correcta*. Si no se establece la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparecerá el mensaje *Error de conexión a la ruta*. Este paso es opcional.

e. En la casilla **Actualizar catálogo**, seleccione **Manual** o **Automático**.
Si el **Catálogo de actualizaciones** se selecciona como**Automáticamente**, seleccione **Diariamente** o **Semanalmente** como la frecuencia de actualización e ingrese la hora en formato de 12 horas.

3. Haga clic en **Finalizar**. El botón **Finalizar** aparece solo después de que ha completado todos los campos en el cuadro de diálogo. Se crea un nuevo catálogo de firmware y se agrega en la tabla Catálogo de la página **Administración de catálogos**.
4. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

Tareas relacionadas

Eliminar un catálogo en la página 79

Información del certificado SSL

Los archivos de catálogo para actualizaciones de firmware y controlador se pueden descargar desde el sitio de soporte de Dell, Dell EMC Repository Manager (Repository Manager) o un sitio web dentro de la red de su organización.

Si decide descargar el archivo de catálogo del sitio web dentro de la red de su organización, puede aceptar o rechazar el certificado SSL. Puede ver los detalles del certificado SSL en la ventana **Información del certificado**. La información se compone del período de validez, la autoridad emisora y el nombre de la entidad para la que se emite el certificado.

NOTA: La ventana **Información del certificado** se muestra únicamente si crea el catálogo desde el asistente **Crear línea de base**.

Acciones

Aceptar	Acepta el certificado SSL y le permite acceder al sitio web.
Cancelar	Cierra la ventana **Información del certificado** sin aceptar el certificado SSL.

Actualizar un catálogo

Los catálogos de firmware y controladores existentes se pueden actualizar desde el sitio Dell.com (ubicación base).

Para actualizar un catálogo, siga estos pasos:

1. En la página Administración de catálogos, seleccione un catálogo.
2. Haga clic en el botón **Comprobación de actualizaciones** ubicado en el panel derecho de la página **Administración de catálogos**.
3. Haga clic en **SÍ.**
Si el catálogo seleccionado es un catálogo en línea, se reemplaza por la versión más actualizada que se mantiene en el sitio Dell.com. Para los catálogos de red local, se consideran todos los firmware y los controladores más recientes disponibles en la ubicación base para medir el nivel de cumplimiento de la base.

Editar un catálogo

1. En la página **Administración de catálogos**, seleccione un catálogo.
Los detalles del catálogo se muestran en el panel derecho **<nombre del catálogo>**.
2. Haga clic en **Editar** en el panel derecho.
3. En el asistente **Editar catálogo de actualización**, edite las propiedades.
Las propiedades que no puede editar aparecen atenuadas. Para obtener información sobre definiciones de campos, consulte Agregar un catálogo con Dell.com en la página 76 y Agregar un catálogo a la red local en la página 77.

4. Ingrese la **Dirección del recurso compartido** y la **Ruta del archivo del catálogo**, aparece el vínculo **Probar ahora**. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se estableció la conexión con el catálogo, aparece un mensaje que indica `Connection Successful`. Si no se ha establecido la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparece el mensaje de error `Connection to path failed`. Este paso es opcional.
5. En la casilla **Actualizar catálogo**, seleccione **Manual** o **Automático**.
   Si el **Catálogo de actualizaciones** se selecciona como**Automáticamente**, seleccione **Diariamente** o **Semanalmente** como la frecuencia de actualización e ingrese la hora en formato de 12 horas.
6. Haga clic en **Finalizar**.
   Se crea y ejecuta inmediatamente un trabajo de detección. El estado del trabajo se indica en la columna **UBICACIÓN DEL REPOSITORIO** de la página **Administración de catálogos**.

Eliminar un catálogo

1. En la página **Administración de catálogos**, seleccione los catálogos y, a continuación, haga clic en **Eliminar**.
   De este modo, se eliminarán los catálogos de la lista.
2. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

NOTA: Los catálogos no se pueden eliminar si están vinculados a una base.

Información relacionada

Agregar un catálogo a la red local en la página 77

Crear una línea de base de firmware o controladores

Una línea de base es un conjunto o grupo de dispositivos que están asociados con un catálogo de firmware o controladores. Se crea una línea de base para la evaluación del cumplimiento del firmware y los controladores para los dispositivos incluidos en esa línea de base en comparación con las versiones especificadas en el catálogo. Para crear una base, siga estos pasos:

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- El Administrador de dispositivos solo puede ver y administrar las líneas de base de firmware o controladores que haya creado ese usuario y que le pertenezcan. Además, durante la creación de líneas de base, se muestran los dispositivos o grupos objetivo (que admiten la actualización del firmware) que solo se encuentran dentro del alcance del administrador de dispositivos.
- Después de actualizar a la versión 3.6, todas las líneas de base de firmware o controladores que hayan creado los administradores de dispositivos desde cualquiera de las versiones anteriores de OpenManage Enterprise se asignan solo al administrador. Por lo tanto, los administradores de dispositivos deben volver a crear las líneas de base de firmware o controladores desde versiones anteriores después de la actualización.
- No se actualizarán automáticamente los dispositivos que no cumplan con una versión del firmware o los controladores que sea anterior a la versión del catálogo. Debe actualizar la versión del firmware. Se recomienda actualizar el firmware de un dispositivo durante las ventanas de mantenimiento para evitar que los dispositivos o el entorno queden sin conexión durante el horario comercial.

1. En **Firmware**, haga clic en **Crear línea base**.
2. En el cuadro de diálogo **Crear base de actualización**:
   a. En la sección **Información de línea base**:
      i. En el menú desplegable **Catálogo**, seleccione un catálogo.
      ii. Para agregar un catálogo a esta lista, haga clic en **Agregar**. Consulte Administración de los catálogos de firmware.
      iii. En la casilla **Nombre de línea base**, ingrese un nombre para la línea base y, a continuación, ingrese una descripción de la línea base.
      iv. Haga clic en **Siguiente**.
   b. En la sección **Destino**:

- Para seleccionar uno o más dispositivos de destino:
  i. Seleccione **Seleccionar dispositivos**, y, a continuación, haga clic en el botón **Seleccionar dispositivos**.
  ii. En el cuadro de diálogo **Seleccionar dispositivos**, todos los dispositivos supervisados por OpenManage Enterprise, los módulos de E/S y los dispositivos en grupos estáticos o de consulta se muestran en los grupos correspondientes.
  iii. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
  iv. Seleccione la casilla de verificación correspondiente a los dispositivos. Los dispositivos seleccionados se indican bajo la pestaña **Dispositivos seleccionados**.
- Para seleccionar uno o más grupos de dispositivos de destino:
  i. Seleccione **Seleccionar grupos**, y, a continuación, haga clic en el botón **Seleccionar grupos**.
  ii. En el cuadro de diálogo **Seleccionar grupos**, todos los dispositivos supervisados por OpenManage Enterprise, los módulos de E/S y los dispositivos en grupos estáticos o de consulta se muestran en las categorías correspondientes.
  iii. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
  iv. Seleccione la casilla de verificación correspondiente a los grupos. Los grupos seleccionados se indican bajo la pestaña **Grupos seleccionados**.

3. Haga clic en **Finish** (Finalizar).
   De este modo, se muestra un mensaje en que se indica que se creó un trabajo para crear la línea base.

   En la tabla Línea base, aparecen los datos sobre el dispositivo y el trabajo de línea base. Para obtener información sobre definiciones de campos, consulte Definiciones de los campos de la línea base de firmware en la página 179.

Eliminación de las bases de cumplimiento de la configuración

Puede eliminar las bases de cumplimiento de la configuración en la página **Configuración** > **Cumplimiento de la configuración** y desvincular los dispositivos de las bases asociadas.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Para eliminar las bases de cumplimiento de la configuración, realice lo siguiente:

1. Seleccione las bases entre las que se enumeran en la página Cumplimiento de la configuración.
2. Haga clic en **Eliminar** y, a continuación, en **Sí** en el mensaje de confirmación.

Las bases de configuración eliminadas se quitan de la página Cumplimiento de la configuración.

Editar una base

Las bases de la página **Configuración** > **Cumplimiento del firmware/controlador** pueden editarse de la siguiente manera:

1. Seleccione una base y, a continuación, haga clic en **Editar** en el panel derecho.
2. Modifique los datos como se describe en Creación de la línea base de firmware.
   La información actualizada se muestra en la lista Línea base.
3. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

Comprobar el cumplimiento del firmware y los controladores de un dispositivo

En la página **Configuración** > **Cumplimiento del firmware/controlador**, puede comprobar el cumplimiento del firmware y de los controladores de los dispositivos de la base en función del catálogo asociado, ver el informe y actualizar el firmware y los controladores de los dispositivos que no cumplen con los requisitos.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- El firmware y los controladores (Windows de 64 bits) para los dispositivos de la base que no cumplen con los requisitos no se actualizan automáticamente, por lo que el usuario debe actualizarlos. Se recomienda actualizar el firmware y los controladores de un dispositivo durante los períodos de mantenimiento para evitar que los dispositivos o el entorno se queden offline durante el horario comercial.
- Para recolectar la información del inventario, el Recolector de inventario y la Actualización del sistema Dell deben estar disponibles en el servidor de Windows. Si estos componentes no están disponibles en el servidor, inicie un trabajo de inventario y seleccione **Recolectar inventario de los controladores**. El trabajo de detección también recolecta información de inventario de los controladores, pero solo el trabajo de inventario instala los componentes necesarios en el servidor. Para recolectar la información del inventario del controlador, cree o edite un trabajo de inventario y seleccione la casilla de verificación **Recolectar inventario de los controladores**. Para obtener más información, consulte Creación de un trabajo de inventario en la página 72 y Edición de un trabajo de programa de inventario en la página 74.

1. Seleccione la casilla de verificación correspondiente a las bases y haga clic en **Comprobar el cumplimiento normativo**.
   Se ejecuta el trabajo de cumplimiento de base.

   NOTA: Si los dispositivos no están relacionados con un catálogo, no se verifica el cumplimiento. Se crea un trabajo solo para los dispositivos que están relacionados y se agregan a la tabla Cumplimiento. Para relacionar un dispositivo con un catálogo, consulte Creación de la línea base de firmware.

   En la tabla Línea base, aparecen los datos sobre el dispositivo y el trabajo de línea base. Para obtener información sobre definiciones de campos, consulte Definiciones de los campos de la línea base de firmware en la página 179.
2. Para ver el informe de cumplimiento y actualizar la versión de firmware y los controladores de los dispositivos, haga clic en **Ver informe** en el panel derecho.

   Consulte Visualización del informe de cumplimiento del firmware del dispositivo.

   NOTA: La reversión no es compatible con los controladores.

Ver el informe de cumplimiento de la base

En la página **Configuración** > **Cumplimiento del firmware/controlador**, se indica el estado de cumplimiento de las bases. El gráfico de anillo proporciona un resumen del cumplimiento de las bases para sus respectivos catálogos. Cuando más de un dispositivo está relacionado con una base, el estado del dispositivo con el nivel de cumplimiento más bajo con respecto a la base se indica como el nivel de cumplimiento de esa base. Por ejemplo, el nivel de cumplimiento de una base aparece como “Crítico” si esta tiene un solo dispositivo cuyo cumplimiento está marcado como “Crítico”,  incluso si la mayoría de los dispositivos está en cumplimiento.

Puede ver el nivel de cumplimiento del firmware y los controladores de los dispositivos individuales relacionados con una base y actualizar la versión del firmware o el controlador en ese dispositivo o cambiarla a una versión anterior. Para ver el informe de cumplimiento de la base, siga estos pasos:

- Seleccione la casilla de verificación correspondiente a la línea base y haga clic en **Ver informe** en el panel derecho.

  En la página **Informe de cumplimiento** aparece la lista de dispositivos relacionados con la línea base y el nivel de cumplimiento. De manera predeterminada, se muestran los dispositivos con estados **Crítico** y **Advertencia**.

  NOTA: Si cada dispositivo tiene su propio estado, el estado de máxima gravedad se considera como el estado del grupo. Para obtener más información sobre el estado de Resumen de condición, consulte las notas técnicas *ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.a GENERACIÓN Y POSTERIORES* en Dell TechCenter.
- **CUMPLIMIENTO**: indica el nivel de cumplimiento de un dispositivo con respecto a la línea base. Para obtener más información sobre los símbolos que se utilizan para analizar los niveles de cumplimiento del firmware o los controladores del dispositivo, consulte Administrar el firmware y los controladores del dispositivo en la página 75.
- **TIPO**: tipo de dispositivo en que se genera el informe de cumplimiento.
- **COMPONENTES Y NOMBRE DEL DISPOSITIVO**: de manera predeterminada, se aparece la etiqueta de servicio del dispositivo.
  1. Para ver información acerca de los componentes del dispositivo, haga clic en el símbolo **>**.

     Aparece una lista de componentes y su cumplimiento con respecto al catálogo.

NOTA: Para todos los dispositivos (excepto el chasis MX7000) que cumplen completamente con los requisitos de la línea de base del firmware asociado, el símbolo **>** no aparece.

2. Seleccione una o varias casillas de verificación correspondientes a los dispositivos cuyo estado de cumplimiento del firmware sea "Crítico" y requieran una actualización.
3. Haga clic en **Hacer compatible**. Consulte Actualizar la versión de firmware del dispositivo usando el informe de cumplimiento de la base.

- **Etiqueta de Servicio**: haga clic en esta opción para ver información detallada sobre el dispositivo en la página **<nombre del dispositivo>**. Para obtener más información sobre las tareas que puede completar en esta página, consulte Ver y configurar dispositivos individuales en la página 67.
- **SOLICITUD DE REINICIO**: indica si el dispositivo se debe reiniciar después de actualizar el firmware.
- **Información** : símbolo correspondiente a cada componente del dispositivo que esté vinculado a la página del sitio de soporte desde la que se puede actualizar el firmware o los controladores. Haga clic en este botón para abrir la página Detalles del controlador correspondiente en el sitio de soporte técnico.
- **VERSIÓN ACTUAL**: indica la versión actual del firmware del dispositivo.
- **VERSIÓN DE BASE**: indica la versión correspondiente del firmware y los controladores del dispositivo disponible en el catálogo asociado.
- Para exportar el informe de cumplimiento a un archivo de Excel, seleccione las casillas de verificación correspondientes con el dispositivo y, a continuación, seleccione **Exportación**.
- Para volver a la página **Firmware**, haga clic en **Volver a firmware**.
- Para ordenar los datos en función de una columna, haga clic en el título de la columna.
- Para buscar un dispositivo en la tabla, haga clic en **Filtros avanzados** y seleccione o ingrese datos en las casillas de filtrado. Consulte la opción Filtros avanzados en Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise en la página 35.

Actualizar el firmware o los controladores con el informe de cumplimiento de la base

Después de ejecutar un informe de cumplimiento de firmware o controlador, si la versión de firmware o controlador en el dispositivo es anterior a la versión en el catálogo, la página Informe de cumplimiento muestra que el estado del firmware o controlador del dispositivo es Actualizar (o).

La versión del firmware y del controlador de los dispositivos asociados de la base no se actualiza automáticamente; por lo tanto, el usuario debe iniciar la actualización. Se recomienda actualizar el firmware o los controladores de un dispositivo durante los períodos de mantenimiento para evitar que los dispositivos o el entorno se queden offline durante el horario comercial.

Los administradores de dispositivos pueden ejecutar la actualización de firmware o controladores únicamente en los dispositivos que se encuentran dentro de su alcance.

NOTA: La recopilación de inventario y la actualización de firmware en los sleds de almacenamiento del chasis no son soportadas en OpenManage Enterprise si se administran a través de la administración de dispositivos del chasis.

Requisitos previos:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Debe crear una regla de firewall entrante para habilitar la comunicación con el puerto 22.
- Si los recursos compartidos HTTP y HTTPS se ajustaron mediante la configuración de proxy, asegúrese de que estas direcciones URL locales se incluyan en la lista de excepciones del proxy antes de iniciar cualquier tarea de actualización.
- Solo se puede iniciar una tarea de actualización en la máquina objetivo en un momento determinado.

NOTA:

- La función Restablecer iDRAC no es compatible con los dispositivos en un chasis MCM que se encuentran en estado de incorporación "Por proxy" y que solo se utilizan para actualizar los controladores de los dispositivos. Para obtener más información sobre los estados de incorporación, consulte Incorporación de dispositivos en la página 44.
- El estado de cumplimiento del firmware o de los controladores de switches de red, IOA modulares y dispositivos Dell Storage se muestra como Desconocido, ya que no se puede actualizar mediante el catálogo Dell. Se recomienda realizar actualizaciones de firmware o controlador individuales para estos dispositivos mediante su paquete de actualización individual correspondiente. Para

realizar actualizaciones de firmware o controlador individuales, seleccione un dispositivo en la página Todos los dispositivos, haga clic en **Ver detalles** > **Firmware/controladores** y seleccione la opción de paquete individual. Para obtener más información sobre la lista de dispositivos no compatibles, consulte Informes de base de cumplimiento del firmware o el controlador: dispositivos con estado de cumplimiento "Desconocido" en la página 183

Si el grupo de administración de chasis múltiples (MCM) se administra con versiones de OpenManage Enterprise-Modular inferiores a la versión 1.30.00, debe tener en cuenta lo siguiente antes de actualizar el firmware o los controladores de los sleds y el chasis de MX7000:

- Las actualizaciones del firmware de chasis y sled deben realizarse por separado.
- El chasis principal debe actualizarse por separado como el paso final después de actualizar todos los chasis miembros.
- El firmware se puede actualizar solo para un máximo de 9 miembros de chasis a la vez.
- La actualización de firmware es compatible con un máximo de 43 sleds a la vez, independientemente del estado de incorporación (Administrado o Por proxy).

Las actualizaciones de controladores solo están disponibles en los dispositivos detectados como servidores de Windows de 64 bits. Antes de actualizar los controladores, realice lo siguiente:

- Tenga en cuenta que no se admite la reversión de las actualizaciones del controlador.
- Las actualizaciones de los controladores dentro de banda solo se admiten en Windows con OpenSSH. No se admiten actualizaciones de controladores en SSH alojados en Windows de otros fabricantes, como el CygwinSSH.
- Para recolectar la información del inventario, el Recolector de inventario y la Actualización del sistema Dell deben estar disponibles en el servidor de Windows. Si estos componentes no están disponibles en el servidor, inicie un trabajo de inventario y seleccione **Recolectar inventario de los controladores**. El trabajo de detección también recolecta información de inventario de los controladores, pero solo el trabajo de inventario instala los componentes necesarios en el servidor. Para recolectar la información del inventario del controlador, cree o edite un trabajo de inventario y seleccione la casilla de verificación **Recolectar inventario de los controladores**. Para obtener más información, consulte Creación de un trabajo de inventario en la página 72 y Edición de un trabajo de programa de inventario en la página 74.

Para actualizar el firmware o controlador de un dispositivo con el informe de cumplimiento de la base, siga estos pasos:

1. En la página **Configuración** > **Cumplimiento del firmware/controlador**, seleccione la casilla de verificación correspondiente a la base a la que el dispositivo está conectado y, a continuación, haga clic en **Ver informe** en el panel de la derecha.

   En la página **Informe de cumplimiento** aparece la lista de dispositivos relacionados con la base y su nivel de cumplimiento. Para obtener descripciones sobre campos, consulte Ver el informe de cumplimiento de la base en la página 81.
2. Seleccione la casilla de verificación correspondiente al dispositivo cuyo firmware o controlador se debe actualizar. Puede seleccionar más de un dispositivo con propiedades similares.
3. Haga clic en **Hacer compatible**.
4. En el cuadro de diálogo **Hacer dispositivos compatibles**, puede hacer lo siguiente:
   - En **Programar actualización**, haga clic en **Información adicional** para ver la información importante y seleccione una de las siguientes opciones:
     a. **Actualizar ahora**: se aplican las actualizaciones del firmware o el controlador inmediatamente.
     b. **Programar más tarde**: seleccione esta opción para especificar una fecha y hora en que se deba actualizar la versión del firmware o el controlador. Este modo se recomienda si no desea alterar sus tareas actuales.
   - En **Opciones del servidor**, seleccione una de las siguientes opciones de reinicio:
     a. Para reiniciar el servidor inmediatamente después de la actualización del firmware o controlador, seleccione **Reiniciar el servidor inmediatamente** y, en el menú desplegable, seleccione una de las siguientes opciones:
        i. **Reinicio ordenado sin apagado forzado**
        ii. **Reinicio ordenado con apagado forzado**
        iii. **Ciclo de encendido y apagado** para un restablecimiento forzado del dispositivo.
     b. Seleccione **Programar para el siguiente reinicio del servidor** a fin de activar la actualización del firmware o el controlador cuando se produzca el siguiente reinicio del servidor.

     NOTA: Si se crean los trabajos de actualización de firmware o controlador con la opción “Programar para el siguiente reinicio del servidor”, se debe ejecutar manualmente la comprobación de la base y el inventario después de instalar el paquete en el dispositivo remoto.
   - **Borrar cola de trabajos:** seleccione esta opción para borrar todos los trabajos (programados, completados y fallidos) antes de que se inicie el trabajo de actualización en el dispositivo objetivo.

     NOTA: Esta función no es compatible con la actualización de los controladores.
   - **Restablecer la iDRAC:** seleccione esta opción para comenzar un reinicio de la iDRAC antes de que se inicie el trabajo de actualización.

     NOTA: Esta función no es compatible con la actualización de los controladores.

5. Haga clic en **Actualizar**.

Se crea un trabajo de actualización de firmware o controlador para actualizar el firmware o el controlador del dispositivo. Puede ver el estado del trabajo en la página **Monitorear** > **Trabajos**.

11

Administrar plantillas de implementación de dispositivos

La plantilla de implementación de dispositivos en OpenManage Enterprise le permite establecer las propiedades de configuración, como BIOS, inicio, propiedades de red, etc. de servidores y chasis.

La plantilla de implementación es una consolidación de los ajustes de configuración del sistema denominados atributos. La plantilla de implementación permite configurar varios servidores o chasis de manera rápida y automática sin el riesgo de que se cometan errores humanos.

Las plantillas le permiten optimizar los recursos de centro de datos y reducir el tiempo de ciclo en la creación de clones e implementaciones. Las plantillas además mejoran sus operaciones de negocios críticas en infraestructura convergente que utilizan infraestructuras definidas por software.

Puede usar las plantillas de implementación predefinidas o importar plantillas de implementación desde un dispositivo de referencia o un archivo de plantilla existente. Para ver la lista de plantillas existentes, en el menú de OpenManage Enterprise, haga clic en **Configuración** > **Plantillas**.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Un administrador de dispositivos puede ver y realizar tareas en las plantillas predeterminadas y las plantillas personalizadas que le pertenezcan.

Temas:

Crear una plantilla de implementación desde un dispositivo de referencia

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184.

Puede crear o editar una plantilla de implementación utilizando un dispositivo de referencia o mediante la importación desde una plantilla de implementación existente. Para crear una plantilla utilizando un dispositivo de referencia realice lo siguiente:

1. En el menú **OpenManage Enterprise**, haga clic en **Configuración** > **Plantillas** > **Crear plantilla** y, luego, seleccione **Desde dispositivo de referencia**.
2. En el cuadro de diálogo **Crear plantilla**:
   a. En la sección **Información de la plantilla**, ingrese un nombre y una descripción para la plantilla de implementación.
   b. Seleccione el tipo de plantilla de implementación:
      - **Clonar servidor de referencia**: le permite clonar la configuración de un servidor existente.
      - **Clonar chasis de referencia**: le permite clonar la configuración de un chasis existente.
      - **Clonar IOA de referencia**: le permite clonar la configuración de un agregador M de I/O existente.
        NOTA: Los atributos en la plantilla de IOA no se pueden editar. Solo se puede editar el **nombre** y la **descripción** de una plantilla de IOA.
   c. Haga clic en **Siguiente**.
   d. En la sección **Dispositivo de referencia**, haga clic en **Seleccionar dispositivo** para seleccionar el dispositivo cuyas propiedades de configuración se deben utilizar para crear la nueva plantilla de implementación. Para obtener más información acerca de la selección de dispositivos, consulte Selección de dispositivos y grupos de dispositivos de destino.
      NOTA: Solo puede seleccionar un dispositivo como dispositivo de referencia.
      NOTA: Solo las plantillas de IOA que se extrajeron en el momento de la detección del chasis están disponibles para la clonación. Consulte Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección en la página 49
   e. En la sección **Elementos de configuración**, seleccione las casillas de verificación correspondientes a los elementos del dispositivo que se deben clonar. Para crear una plantilla de implementación utilizando un servidor como dispositivo, puede seleccionar clonar las propiedades del servidor, como iDRAC, BIOS, Lifecycle Controller y Filtros de eventos. De forma predeterminada, se seleccionan todos los elementos.
   f. Haga clic en **Finalizar**.
      Después de que la creación se haya completado correctamente, el trabajo se muestra en la lista. Se inicia un trabajo de creación de plantillas de implementación y el estado se muestra en la columna **ESTADO**.

      La información del trabajo también se muestra en la página **Monitorear** > **Trabajos** Para ver información adicional sobre el trabajo, selecciónelo y, luego, haga clic en **Ver detalles** en el panel de trabajo. En la página **Detalles del trabajo**, aparecen los detalles de ejecución del trabajo. En el panel **Resultados**, haga clic en **Ver detalles** para ver información detallada de la ejecución del trabajo.

Crear una plantilla de implementación importando un archivo de plantilla

NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.

1. En el menú **OpenManage Enterprise**, haga clic en **Configuración** > **Plantillas** > **Crear plantilla** y, luego, seleccione **Importar desde archivo**.
2. En el cuadro de diálogo **Importar plantilla**:
   a. Introduzca un nombre para la nueva plantilla de implementación.
   b. Haga clic en **Seleccionar un archivo** y, a continuación, seleccione un archivo de plantilla.
   c. Seleccione **Servidor**, **Chasis** o **IOA** para indicar el tipo de plantilla.
3. Haga clic en **Finalizar**.
   Las propiedades de un archivo de plantilla existente se importan y se crea una plantilla de implementación nueva.

- Para ver la información de una plantilla de implementación, seleccione la casilla de verificación y, a continuación, haga clic en **Ver detalles** en el panel derecho. En la página **Detalles de la plantilla**, puede implementar o editar una plantilla de implementación.

Consulte Implementar las plantillas de implementación de dispositivos en la página 90 y Crear una plantilla de implementación desde un dispositivo de referencia en la página 85.

- Para editar una plantilla de implementación:
  1. Seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Editar**.
  2. En el cuadro de diálogo **Editar plantilla**, edite el nombre de la plantilla de implementación y, a continuación, haga clic en **Finalizar**. La información actualizada se muestra en la lista de plantillas de implementación.

Ver la información de una plantilla de implementación

Una lista de plantillas de implementación de dispositivo predefinidas, creadas por usuarios o clonadas aparece en **Configuración** > **Plantillas**.

1. En la lista de plantillas de implementación, seleccione la casilla de verificación correspondiente a la plantilla de dispositivo requerida.
2. En el panel de trabajo, haga clic en **Ver detalles**.
   En la página **Detalles de la plantilla**, aparece el nombre de la plantilla de implementación, su descripción, el dispositivo de referencia del cual se creó la plantilla de implementación e información de la fecha de última actualización por parte del usuario de OpenManage Enterprise.
3. Haga clic con el botón derecho en un elemento para expandir o contraer todos los elementos secundarios de la sección **Detalles de configuración** y mostrar todos los atributos que se utilizan para crear la plantilla de implementación. También puede expandir cada uno de los elementos secundarios específicos de un elemento principal. Por ejemplo, si seleccionó que los elementos de iDRAC y BIOS deben usarse para la clonación en el dispositivo de destino, solo se muestran los atributos relacionados con esos elementos.

Editar una plantilla de implementación de servidor

No se pueden editar las plantillas de implementación incorporadas. Solo se pueden editar las plantillas de implementación creadas por el usuario que se identifican como "personalizadas". Puede editar los atributos de una plantilla de implementación independientemente de si se creó por medio de un archivo de plantilla de referencia o un dispositivo de referencia.

1. En la página **Plantillas de** > **cumplimiento**, seleccione la casilla de verificación obligatoria correspondiente y, luego, haga clic en **Editar**.
2. En el cuadro de diálogo **Editar plantilla**:
   a. En la sección **Información de la plantilla**, edite el nombre y la descripción de la plantilla de implementación. No se puede editar el tipo de plantilla.
   b. Haga clic en **Siguiente**.
   c. En la sección **Editar Componentes**, los atributos de la plantilla de implementación se muestran en:
      - La **Vista guiada**: esta vista de atributos muestra solo atributos comunes, agrupados por función. Se muestran atributos de las siguientes categorías:
        i. En la sección **Configuración del BIOS**, seleccione una de las opciones siguientes:
           - **Manualmente**: permite definir manualmente las siguientes propiedades del BIOS:
             - **Perfil del sistema**: en el menú desplegable, seleccione esta opción para especificar el tipo de optimización de rendimiento que se debe lograr en el perfil del sistema.
             - **Puertos USB accesibles para el usuario**: en el menú desplegable, seleccione esta opción para especificar los puertos a los que puede acceder el usuario.
             - De manera predeterminada, están activados el uso del procesador lógico y la capacidad de administración en banda.
           - **Optimizar según la carga de trabajo**: en el menú desplegable, seleccione perfil de carga de trabajo, seleccione para especificar el tipo de optimización de rendimiento de la carga de trabajo que desea lograr en el perfil.
        ii. Haga clic en **Arranque** y defina el modo de arranque:
           - Si selecciona el BIOS como el modo de arranque, haga lo siguiente:
             - Para reintentar la secuencia de arranque, seleccione la casilla de verificación **Activado**.
             - Arrastre los elementos para establecer la secuencia de arranque y la secuencia de la unidad de disco duro.
           - Si selecciona UEFI como el modo de arranque, arrastre los elementos para establecer la secuencia de arranque de UEFI. Si es necesario, seleccione la casilla de verificación para activar la función Secureboot.
        iii. Haga clic en **Redes**. Todas las redes asociadas con la plantilla de implementación se muestran en las **Interfaces de red**.
           - Para asociar un grupo de identidad opcional con la plantilla de implementación, seleccione en el menú desplegable el **grupo de identidad**. Se muestran las redes asociadas con el grupo de identidad seleccionado. Si la plantilla de implementación se edita en la vista Avanzada, se desactiva la selección del grupo de identidad para esta plantilla de implementación.
             - Para ver las propiedades de la red, amplíe la red.

- Para editar las propiedades, haga clic en el símbolo de lápiz correspondiente.
  - Seleccione el protocolo que se debe utilizar para el arranque. Seleccione solo si el protocolo es compatible con la red.
  - Seleccione la red etiquetada y no etiquetada que se debe asociar a la red
  - En la plantilla de implementación (perfil) creada anteriormente se muestran la partición, el ancho de banda máximo y mínimo.
- Haga clic en **Finalizar**. Se guarda la configuración de red de la plantilla de implementación.

- La **Vista avanzada**: esta vista muestra todos los atributos de plantilla de implementación que se pueden cambiar (incluidos los que se muestran en la Vista guiada). Esta vista le permite especificar no solo valores de atributo (como en la Vista guiada), sino que también si cada atributo se incluye o no cuando se implementa la plantilla de implementación en un dispositivo de destino.

  Los atributos se agrupan según su función para verlos mejor. Los atributos específicos del proveedor se agrupan en Otros atributos. Cada atributo individual se muestra con una casilla de verificación antes del nombre. La casilla de verificación indica si el atributo se incluirá o no cuando se implemente la plantilla de implementación en un dispositivo de destino. Debido a las dependencias de atributos, si cambia la configuración de si se implementa o no un atributo en particular, podrían producirse resultados inesperados en el dispositivo de destino o hacer que la implementación falle. Cada grupo también tiene una casilla de verificación a la izquierda de su nombre. El ícono en las casillas de verificación de grupo tiene uno de estos tres valores:

  i. Seleccionada: Indica que todos los atributos del grupo están seleccionados para la implementación.
  ii. Guion: Indica que se seleccionaron algunos de los atributos (pero no todos) para la implementación.
  iii. Sin marca: Indica que ninguno de los atributos del grupo está seleccionado para la implementación

  NOTA:
  - Debe tener cuidado y conocer bien los atributos y las dependencias de atributos cuando utilice esta opción, ya que varios atributos dependen del valor de otro atributo para determinar su comportamiento.
  - Puede hacer clic en los íconos de grupo para alternar la configuración de implementación para todos los atributos del grupo.
  - Los atributos con información segura, como las contraseñas, están ocultos y se muestran como “vacíos” cuando se cargan inicialmente, y se enmascaran los cambios en estos valores de atributos seguros.
  - No se puede cambiar el grupo de identidades asociado de una plantilla de implementación si ya hay un perfil asociado a él.

3. Haga clic en **Siguiente**.
   En la sección **Resumen**, se muestran los atributos que editó utilizando los modos Guiado y Avanzado.
4. Esta sección es de solo lectura. Lea la configuración y haga clic en **Finalizar**.
   Los atributos de la plantilla actualizada se guardan en la plantilla de implementación.

Editar una plantilla de implementación de chasis

Es posible editar plantillas de implementación de chasis con OpenManage Enterprise.

NOTA:
- Para editar plantillas de implementación de chasis, debe tener privilegios de administrador o de administrador de dispositivos. Para obtener más detalles, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Las contraseñas de usuario no se pueden establecer en el chasis MX7000 y las plantillas de implementación de Chassis Management Controller (CMC).

Para editar una plantilla de implementación de chasis:

1. Seleccione **OpenManage Enterprise** > **Configuración** > **Plantillas** para obtener una lista de plantillas de implementación.
2. Seleccione la casilla de verificación que corresponda a la plantilla de chasis requerida y haga clic en **Editar**. Asegúrese de que la plantilla de implementación esté identificada como "Personalizada".
3. Edite el **Nombre de la plantilla** y la **Descripción** en la sección **Información de la plantilla**. El **tipo de plantilla** no se puede editar.
4. Haga clic en **Siguiente**.
5. En la sección **Editar componentes** en **Vista avanzada**, puede seleccionar o anular la selección de los atributos que desea incluir en la plantilla de implementación o excluir de ella.
6. Haga clic en **Siguiente**.
7. Puede revisar los cambios en los atributos en **Resumen**. Aparece un círculo junto a los atributos modificados.
8. Haga clic en **Finalizar** para guardar los cambios en la plantilla de implementación de chasis.

Editar una plantilla de implementación de IOA

Los atributos en la plantilla de implementación de IOA no se pueden editar. Solo se puede editar el **nombre** y la **descripción** de una plantilla de implementación de IOA.

NOTA:

Los atributos de la plantilla de IOA no se deben editar fuera del dispositivo porque la plantilla se considerará un archivo corrupto durante la implementación.

Editar las propiedades de red de una plantilla de implementación

En la página **Configuración** > **Plantillas**, puede editar la configuración de red de las plantillas de implementación que contengan los atributos de la NIC correspondientes.

Después de seleccionar una plantilla de implementación, haga clic en **Editar red** para activar el asistente de edición de red y realice lo siguiente:

NOTA: Los ajustes de VLAN en los sleds MX7000 “por proxy” dentro del alcance están permitidos para un administrador de dispositivos, incluso si el chasis MX7000 está fuera del alcance.

1. Haga clic en **Asignación del pool de I/O** y, en la lista **Pool de identidades**, seleccione un pool de identidades para la plantilla de implementación. Haga clic en **Siguiente**.
2. En la sección **Ancho de banda**, edite el **Ancho de banda mínimo (%)** y el **Ancho de banda máximo (%)** de las NIC asociadas y haga clic en **Siguiente**.

   NOTA: Los ajustes del ancho de banda solo se aplican a las NIC con particiones.

3. En la sección **VLAN** (se aplica solo a los sistemas modulares):
   a. Seleccione una opción apropiada de **Formación de equipos NIC**.
   b. Seleccione la casilla de verificación **Propagar los ajustes de la VLAN inmediatamente** para propagar los ajustes de la VLAN modificados en los servidores del sistema modular asociado inmediatamente sin necesidad de reiniciar el servidor. Haga clic en **Ver detalles** para ver los dispositivos que se verán afectados.

      NOTA:

      - **Propagar los ajustes de la VLAN inmediatamente** se implementa solo si la plantilla de implementación ya se ha implementado.
      - Antes de propagar la configuración de VLAN, asegúrese de que los perfiles de red ya se hayan creado para los servidores de sistema modular en el fabric.
      - Si la casilla de verificación **Propagar los ajustes de la VLAN inmediatamente** está seleccionada, entonces se crea un trabajo denominado **Propagación de VLAN** para aplicar los cambios. El estado del trabajo se puede comprobar en la página **Monitorear** > **Trabajos**.

   c. Seleccione la casilla de verificación **Usar comprobación estricta** para hacer coincidir las VLAN con características similares. Si no está seleccionada, solo se usan el nombre de VLAN y QoS para fines de coincidencia.

      NOTA: Esta opción se aplica solo a los sled de sistema modular.

   d. Realice los cambios en los atributos de **Red sin etiqueta** y la **Red etiquetada** de las NIC asociadas, según sea necesario.
4. Haga clic en **Finalizar** para aplicar los cambios.

Implementar las plantillas de implementación de dispositivos

Puede implementar una plantilla de implementación que incluya un conjunto de atributos de configuración para dispositivos específicos. La implementación de una plantilla de implementación de dispositivos en los dispositivos asegura que los dispositivos se configuren de manera uniforme.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Si un administrador de dispositivos está implementando plantillas, solo se muestran los dispositivos y grupos objetivo que se encuentran dentro del alcance del administrador de dispositivos y que son compatibles con la implementación.

Antes de comenzar a implementar una plantilla de implementación de dispositivos, asegúrese de que:

- Ha creado una plantilla de implementación de dispositivos o clonado una plantilla de implementación ejemplo. Consulte Crear una plantilla de implementación desde un dispositivo de referencia en la página 85.
- Los dispositivos de destino cumplen con los requisitos especificados en Requisitos mínimos del sistema para implementar OpenManage Enterprise en la página 21.
- La licencia de OpenManage Enterprise Advanced está instalada en los dispositivos de destino.

PRECAUCIÓN: Asegúrese de que se seleccionen solo los dispositivos apropiados para la implementación. Después de implementar una plantilla de implementación en un dispositivo vacío y de reasignación, es posible que no se pueda revertir el dispositivo a su configuración original.

NOTA: Durante la implementación de una plantilla de chasis MX7000:

- El dispositivo de destino solo puede ser el chasis principal MX7000.
- Si se elimina un chasis MX7000 del grupo, se debe volver a detectar en OpenManage Enterprise.
- Los usuarios en el chasis MX7000 se reemplazan por los usuarios configurados en la plantilla.
- La configuración importada de Active Directory se reemplaza por los valores en el perfil del chasis.

1. En la lista de plantillas de implementación la página **Plantillas de** > **configuración**, seleccione la casilla de verificación que corresponde a la plantilla de implementación que desea implementar y haga clic en **Implementar plantilla**.
2. En el cuadro de diálogo **Implementar plantilla: <template_name>**, en **Destino**:
   a. Haga clic en **Seleccionar** y, a continuación, seleccione dispositivos en el cuadro de diálogo **Destino del trabajo**. Consulte Selección de dispositivos y grupos de dispositivos destino.
   b. Durante la implementación de la plantilla de implementación de dispositivos, es posible que los cambios en la configuración requieran un reinicio forzado del servidor. Si no desea reiniciar el servidor, seleccione la opción **No reiniciar de manera forzada el SO del host**.
   Se intenta realizar un reinicio estable del servidor cuando se selecciona la opción **No reiniciar de manera forzada el SO del host**. Si el reinicio falla, deberá volver a ejecutar la tarea de implementación de la plantilla.
   c. Seleccione la casilla de verificación **Usar comprobación estricta** para hacer coincidir las VLAN con características similares. Si no está seleccionada, solo se usan el nombre de VLAN y QoS para fines de coincidencia

      NOTA: Esta opción solo se muestra si los dispositivos de destino seleccionados son sleds de sistema modular.

   d. Haga clic en **Siguiente**.
3. Si el dispositivo de destino es un servidor, en la sección **Arrancar desde ISO de red**:
   a. Seleccione la casilla de verificación **Inicio para la imagen ISO de red**.
   b. Seleccione **CIFS** o **NFS** como tipo de recurso compartido y, luego, ingrese la información en los campos, como la ruta del archivo de imagen ISO y la ubicación del recurso compartido en el que se almacenará el archivo de imagen ISO. Utilice la información sobre herramientas para ingresar la sintaxis correcta.
   c. Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.
   d. Haga clic en **Siguiente**.
4. En la sección **IP de administración de iDRAC**, cambie la configuración de IP del dispositivo objetivo, si es necesario, y haga clic en **Siguiente**.

   NOTA:

- La implementación de la plantilla falla si se asignan ajustes de DHCP durante la implementación de plantilla en un dispositivo de destino que se descubrió originalmente mediante una IP estática.
- Si los ajustes de IP no están configurados en el sled MX7000 detectado, la operación Arrancar desde ISO de red no se ejecuta durante la implementación de la plantilla.

5. En la sección **Atributos de destino**, los atributos de identidad no virtuales específicos de cada uno de los dispositivos de destino seleccionados, como los atributos de ubicación y la dirección IP, se pueden modificar antes de implementar la plantilla de implementación. Cuando se implementa la plantilla, estos atributos del objetivo modificados se implementan solo en los dispositivos específicos. Para cambiar los atributos de identidad no virtuales específicos del dispositivo:
   a. Seleccione un dispositivo objetivo de la lista que muestra los dispositivos objetivo seleccionados anteriormente.
   b. Expanda las categorías de atributos y, luego, seleccione o anule la selección de los atributos que deben incluirse o excluirse durante la implementación de la plantilla en el dispositivo objetivo.
   c. Haga clic en **Siguiente**.
6. En la sección **Identidades virtuales**, haga clic en **Identidades reservadas**.
   Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
   NOTA: Si las identidades ya están asignadas fuera del dispositivo, una implementación nueva no utilizará esas identidades, a menos que se borren. Para obtener más información, consulte Grupos de identidades en la página 95
7. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte Definiciones de los campos Programar trabajos en la página 179.
8. Haga clic en **Finish** (Finalizar). Revise el mensaje de advertencia y haga clic en **SÍ**.
   Se crea un trabajo de configuración de dispositivo. Consulte Utilización de trabajos para el control de dispositivos en la página 128.

Implementar plantillas de implementación de IOA

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Antes de comenzar a implementar una plantilla de implementación de IOA, asegúrese de lo siguiente:

- Creó una plantilla de implementación de IOA para la implementación. Consulte Crear una plantilla de implementación desde un dispositivo de referencia en la página 85.
- Los dispositivos de destino cumplen con los requisitos especificados en Requisitos mínimos del sistema para implementar OpenManage Enterprise en la página 21.
- La versión de firmware del dispositivo de destino es la misma que la de la plantilla de implementación de IOA.
- Solo se admiten las siguientes implementaciones entre plantillas:

Tabla 14. Implementaciones compatibles entre plantillas

Modo de plantilla de implementación de IOA	Modos de plantilla de IOA de destino admitidas
Independiente	Independiente, PMUX
PMUX (MUX programable)	PMUX, independiente
VLT	VLT

PRECAUCIÓN: Asegúrese de que se seleccionen solo los dispositivos apropiados para la implementación. Después de implementar una plantilla de implementación en un dispositivo vacío y de reasignación, es posible que no se pueda revertir el dispositivo a su configuración original.

1. En la lista de plantillas de implementación de la página **Configuración** > **Plantillas**, seleccione la casilla de verificación que corresponde a la plantilla de IOA que desea implementar y haga clic en **Implementar plantilla**.
2. En el cuadro de diálogo **Implementar plantilla: <template_name>**, en **Destino**:
   a. Haga clic en **Seleccionar** y, a continuación, seleccione dispositivos en el cuadro de diálogo **Destino del trabajo**. Consulte Selección de dispositivos y grupos de dispositivos destino.
   b. Haga clic en **Aceptar**.
3. En el cuadro de diálogo **Nombres de host**, puede cambiar el **nombre del host** del dispositivo de IOA de destino. Haga clic en **Siguiente**.

4. En el cuadro de diálogo **Opciones avanzadas**, seleccione el **Modo de vista previa** para simular la implementación, o seleccione **Continuar con la advertencia** para implementar la plantilla y no considerar las advertencias que se presenten. Haga clic en **Siguiente**.
5. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte Definiciones de los campos Programar trabajos en la página 179.
6. Haga clic en **Finish** (Finalizar). Revise el mensaje de advertencia y haga clic en **SÍ**.
   Un trabajo de configuración de dispositivo se crea en Trabajos. Consulte Utilización de trabajos para el control de dispositivos en la página 128.

Clonar plantillas de implementación

1. En el menú **OpenManage Enterprise**, en **Configuración**, haga clic en **Plantillas**.
   Se muestra una lista de plantillas de implementación disponibles.
2. Seleccione la casilla de verificación correspondiente a la plantilla que desea clonar.
3. Haga clic en **Clonar**.
4. Ingrese el nombre de la plantilla de implementación nueva y, a continuación, haga clic en **Finalizar**.
   La plantilla de implementación clonada se crea y se muestra en la lista de plantillas de implementación.

Implementación automática de la configuración en servidores o chasis que aún no se han descubierto

Las plantillas de implementación existentes en OpenManage Enterprise se pueden asignar a los servidores y chasis que están en espera de ser descubiertos. Estas plantillas de implementación se implementan automáticamente en los respectivos dispositivos cuando estos se descubren e incorporan.

Para acceder a la página **Implementación automática**, haga clic en **OpenManage Enterprise** > **Configuración** > **Implementación automática**.

Se muestran los destinos de la implementación automática y el respectivo **identificador**(etiqueta de servicio o los ID de nodo), **nombre de la plantilla**, **tipo de plantilla**, **estado** y **arranque para el estado ISO de red** (para servidores).

La lista de destinos de **Implementación automática** se puede personalizar mediante los campos **Filtros avanzados** que se encuentran en la parte superior de la lista.

En la sección del costado derecho de la página Implementación automática, se muestran los detalles **Creados en** y **Creado por** del destino de implementación automática seleccionado. Cuando se seleccionan varios elementos, en la sección se muestran los detalles del último elemento seleccionado.

Una vez que se descubre un objetivo de implementación automática, su entrada desde la página Implementación automática se elimina automáticamente y se transfiere a la página Todos los dispositivos. Además, se crea un perfil en la página Perfiles que contiene los valores de configuración del dispositivo.

Se pueden llevar a cabo las siguientes acciones en la página de implementación automática:

- **Crear** plantillas para la implementación automática. Consulte Crear destinos de implementación automática en la página 93
- **Eliminar** plantillas innecesarias. ConsulteEliminar destinos de implementación automática en la página 94
- **Exportar** la plantilla de implementación automática a diferentes formatos. Consulte Exportar detalles del destino de implementación automática a diferentes formatos en la página 94

NOTA:

- Solo los administradores pueden realizar las tareas de creación, eliminación y exportación en las plantillas de implementación automática. Los administradores de dispositivos solo pueden "exportar" las plantillas de implementación automática. Para obtener más información, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Crear destinos de implementación automática

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Para crear destinos de implementación automática:

1. Haga clic en **OpenManage Enterprise** > **Configuración** > **Implementación automática** > **Crear**
   Aparece el asistente de **Implementación automática de plantilla**.
2. En la página **Información de la plantilla**, seleccione el tipo de plantilla de implementación (Servidor o Chasis).
3. En el menú desplegable **Seleccionar Plantilla**, seleccione una plantilla correspondiente. Si la plantilla seleccionada tiene los atributos de identidad que no están asociados con un pool de identidades virtuales, se muestra el siguiente mensaje: *la plantilla seleccionada tiene atributos de identidad, pero no se ha asociado con un pool de identidades virtuales. La implementación de esta plantilla no cambiará las direcciones de red virtual en los dispositivos de destino.*
4. Haga clic en Siguiente.
   Se muestra la página **Información de destino**.
5. En la página **Información del destino**, se pueden seleccionar los dispositivos de destino en uno de los siguientes métodos:
   - **Introducir manualmente:** ingrese la etiqueta de servicio o los ID de nodo para identificar los dispositivos de destino. Los identificadores se pueden introducir en cualquier orden, sin embargo, los identificadores se deben separar por comas. Haga clic en Validar para verificar la precisión de los valores. Es obligatorio para validar los identificadores.
   - **Importar CSV**: haga clic en **Importar CSV** para navegar por las carpetas y seleccionar el archivo .csv respectivo con los detalles del dispositivo de destino. Se muestra un resumen del número de entradas importadas correctamente y no válidas. Para obtener una vista más detallada del resultado de la importación, haga clic en **Ver detalles**.

     Las entradas en el archivo CSV deben tener el siguiente formato: los identificadores se deben incluir en la lista en la primera columna, uno por fila, comenzando desde la segunda fila. Para obtener una plantilla de archivo CSV, haga clic en **Descargar archivo CSV de muestra**.
6. Haga clic en **Siguiente**.
7. En la página **Información de grupo de destino**, especifique un subgrupo en el **Grupo estático**, si está disponible. Para obtener más información sobre el agrupamiento de dispositivos, consulte Organizar los dispositivos en grupos en la página 54. Los dispositivos de destino se colocarían en el grupo de destino especificado en el momento del descubrimiento
8. Haga clic en **Siguiente**.
9. Si el dispositivo de destino es un servidor, en la página **Arrancar desde ISO de red**:
   - Seleccione la casilla de verificación **Inicio para la imagen ISO de red**.
   - Seleccione **CIFS** o **NFS**.
   - Ingrese la **Ruta ISO** de ubicación en la que se almacenó el archivo de imagen ISO. Utilice la información sobre herramientas para ingresar la sintaxis correcta.
   - Ingrese **Dirección IP de recurso compartido**, **Grupo de trabajo**, **Nombre de usuario** y **contraseña**.
   - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.
   - Haga clic en **Siguiente**.
10. En la página **Identidades virtuales**, haga clic en **Identidades reservadas**.
    Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
11. En la sección **Atributos de destino**, los atributos de identidad no virtuales específicos de cada uno de los dispositivos de destino seleccionados, como los atributos de ubicación y la dirección IP, se pueden modificar antes de implementar la plantilla de implementación. Cuando se implementa la plantilla, estos atributos del objetivo modificados se implementan solo en los dispositivos específicos. Para cambiar los atributos de identidad no virtuales específicos del dispositivo:
    a. Seleccione un dispositivo objetivo de la lista que muestra los dispositivos objetivo seleccionados anteriormente.
    b. Expanda las categorías de atributos y, luego, seleccione o anule la selección de los atributos que deben incluirse o excluirse durante la implementación de la plantilla en el dispositivo objetivo.
    c. Haga clic en **Siguiente**.
12. Haga clic en **Finish** (Finalizar).
    Mensaje de alerta *Es posible que la implementación de una plantilla cause la pérdida de datos y un reinicio del dispositivo. ¿Está seguro de que desea implementar la plantilla?* aparece en la pantalla.
13. Haga clic en **Sí**.
    En la página **Implementación automática** se crea y se indica un nuevo destino de implementación automática.

Eliminar destinos de implementación automática

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

NOTA: Si una plantilla asociada a destinos de implementación automática se elimina de la página **OpenManage Enterprise** > **Configuración** > **Plantillas**, las entradas de implementación automática asociadas también se eliminarían independientemente del estado actual.

Para quitar los destinos de la implementación automática de la lista de **Implementación automática**.

1. Vaya a la página de implementación automática haciendo clic en **OpenManage Enterprise** > **Configuración** > **Implementación automática**.
2. Seleccione los destinos de implementación automática en la lista.
3. **Eliminar** y, a continuación, haga clic en **Sí** para confirmar.
   Los destinos de implementación automática que se seleccionan para su eliminación, se eliminan de la página de implementación automática.

Exportar detalles del destino de implementación automática a diferentes formatos

1. Vaya a la página de implementación automática haciendo clic en **OpenManage Enterprise** > **Configuración** > **Implementación automática**.
2. Seleccione el destino de implementación automática en la lista y haga clic en **Exportar**.
3. En el cuadro de diálogo **Exportar todos**, seleccione formato como HTML, CSV o PDF. Haga clic en **Finalizar**.
   Se crea un trabajo y los datos de destino de implementación automática se exportan en el formato seleccionado.

Descripción general de la implementación sin estado

Para implementar una plantilla de implementación de dispositivo con atributos de identidades virtuales en los dispositivos de destino, realice lo siguiente:

1. **Crear una plantilla de dispositivos:** haga clic en la tarea **Crear plantilla** en la pestaña **Implementar** para crear una plantilla de implementación. Puede seleccionar para crear la plantilla desde un archivo de configuración o un dispositivo de referencia.
2. **Cree un grupo de identidades**: haga clic en la tarea **Crear**, en la pestaña **Grupos de identidades**, para crear un grupo de uno o varios tipos de identidades virtuales.
3. **Asigne identidades virtuales a una plantilla de dispositivo**: seleccione una plantilla de implementación en el panel **Plantillas** y haga clic en **Editar red** para asignar un grupo de identidades a la plantilla de implementación. También puede seleccionar la red etiquetada y no etiquetada, y asignar el ancho de banda mínimo y máximo a los puertos.
4. **Implemente la plantilla de implementación en dispositivos de destino**: utilice la tarea **Implementar plantilla** en la pestaña **Implementar** para implementar la plantilla de implementación y las identidades virtuales en los dispositivos de destino.

Administrar grupos de identidades: implementación sin estado

La E/S interfaces de un servidor, como, por ejemplo, HBA o NIC, que tienen los atributos de la identidad única que se asignan por el fabricante de las interfaces. Estos exclusivo los atributos de la identidad se conocen generalmente como la identidad de E/S de un servidor. La E/S identidades identificar de forma exclusiva un servidor en una red y también determinan el modo el servidor se comunica con un recurso de red mediante un protocolo específico. Mediante OpenManage Enterprise, puede generar automáticamente y asignar los atributos de identidad virtuales a las interfaces de E/S de un servidor.

A los servidores implementados mediante una plantilla de implementación de dispositivos que contiene identidades de E/S virtuales se los conoce como "sin estado". Las implementaciones sin estado le permiten crear un entorno de servidor dinámico y flexible. Por ejemplo, si implementa un servidor con identidades de E/S virtuales en un entorno de inicio desde SAN puede realizar rápidamente las siguientes tareas:

- Reemplazar un servidor que ha fallado o que falla mediante la transferencia de la identidad de E/S del servidor a otro servidor de repuesto.
- Implementar servidores adicionales para aumentar la capacidad de cálculo durante los procesos de mayor carga de trabajo.

En la página **OpenManage Enteprise** > **Configuración** > **Pools de identidades**, puede crear, editar, eliminar o exportar grupos de E/S virtuales.

NOTA:
- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Las restricciones basadas en el alcance no se aplican a los pools de identidades; por lo tanto, todos los tipos de usuarios pueden ver y utilizar todos los pools de identidades. Sin embargo, una vez que un administrador de dispositivos asigne las identidades, ese administrador de dispositivos solo podrá ver y usar esas identidades.

Crear grupo de identidades: información del grupo

Los grupos de identidades se utilizan para la implementación basada en plantillas en servidores con el fin de virtualizar la identidad de la red para lo siguiente:
- Ethernet
- iSCSI
- Fibre Channel sobre Ethernet (FCoE)
- Fibre Channel (FC)

Puede crear un máximo de 5000 grupos de identidades en cada una de estas categorías.

El proceso de implementación en servidores captura la siguiente identidad disponible en el grupo y la utiliza durante el aprovisionamiento de un servidor a partir de la descripción de la plantilla. A continuación, puede migrar el perfil de un servidor a otro sin perder acceso a la red o almacenar recursos en su entorno.

Puede editar el número de entradas del grupo. Sin embargo, no puede reducir el número de entradas por debajo de las que haya asignadas o reservadas. También puede eliminar las entradas que no estén asignadas o reservadas.

Grupos de identidades

Un bloque de identidades es un conjunto de uno o varios tipos de identidades virtuales que se requieren para la comunicación de red. Un grupo de identidades puede contener una combinación de cualquiera de los siguientes tipos de identidades:
- Identidades de Ethernet

  Las identidades de Ethernet definidas por la dirección de control de acceso al medio (MAC). Las direcciones MAC son necesarias para las comunicaciones de Ethernet (LAN).
- Identidades de iSCSI

  Las identidades definidas por el nombre calificado iSCSI (IQN). Las identidades de IQN son necesarias para admitir el inicio desde SAN por medio del protocolo iSCSI.
- Identidades de Fibre Channel (FC)

  Las identidades definidas por el nombre de nodo mundial (WWNN) y el nombre de puerto de ámbito mundial (WWPN). UN WWNN identidad está asignado a un nodo (dispositivo) en una red fabric FC y puede ser compartida por algunos o todos los puertos de un dispositivo. UN WWPN identidad está asignada a cada puerto en una red fabric FC y es único para cada puerto. WWNN y el WWPN identidades son necesarios para admitir boot-from-SAN y para acceso a los datos mediante FC y Canal de fibra sobre Ethernet (FCoE) protocolos.
- Identidades de Fibre Channel por Ethernet (FCoE)

  Identidades que proporcionan una identidad virtual única para las operaciones de FCoE. La dirección MAC y las direcciones de FC (es decir, WWNN y WWPN) definen estas identidades. WWNN y el WWPN identidades son necesarios para admitir boot-from-SAN y para acceso a los datos mediante FC y Canal de fibra sobre Ethernet (FCoE) protocolos.

OpenManage Enterprise utiliza los grupos de identidades para asignar automáticamente identidades virtuales a la plantilla de implementación de dispositivos que se utiliza para implementar un servidor.

NOTA:

- Para las identidades que pertenecen a un grupo de identidades existente, pero que se implementaron fuera de OpenManage Enterprise, se debe iniciar un nuevo trabajo de inventario de configuración para identificarlos y designarlos como “asignados” en el dispositivo.
- Las identidades virtuales que ya están asignadas no se utilizarán para una implementación nueva, a menos que se borren estas identidades.

Crear grupos de identidades

Puede crear un grupo de identidades que contenga uno o varios tipos de identidades virtuales. Todos los administradores de dispositivos pueden utilizar el pool común que creó el administrador. Además, el administrador puede ver todas las identidades en las cuales se utiliza. Los administradores de dispositivos pueden ver todos los pools de identidades y realizar todas las operaciones en ellos (según se especifica en el Control de acceso basado en funciones o RBAC), mientras que, en la sección Uso, los administradores de dispositivos solo pueden ver las identidades asociadas a los dispositivos que se encuentran dentro de su alcance.

Para crear un grupo de tipos de identidades virtuales:

1. En la página **Configuración**, haga clic en **Grupos de identidades**.
2. Haga clic en **Crear**.
3. En el cuadro de diálogo **Crear grupos de identidades**, en **Información del grupo**:
   a. Ingrese un nombre único para el grupo de identidades y una descripción apropiada.
   b. Haga clic en **Siguiente**.
4. En la sección **Ethernet**:
   a. Seleccione la casilla de verificación **Incluir direcciones MAC virtuales Ethernet** para incluir las direcciones MAC.
   b. Ingrese una dirección MAC de inicio y especifique la cantidad de identidades MAC virtuales que se debe crear.
5. En la sección **iSCSI**:
   a. Seleccione la casilla de verificación **Incluir direcciones MAC iSCSI** para incluir las direcciones MAC iSCSI.
   b. Ingrese una dirección MAC de inicio y especifique la cantidad de direcciones MAC iSCSI que se debe crear.
   c. Seleccione **Configurar el iniciador iSCSI** y, a continuación, especifique el prefijo IQN.
   d. Seleccione **Activar grupo de IP del iniciador iSCSI** y, a continuación, ingrese los detalles de la red.

   NOTA: El grupo de IP del iniciador iSCSI no es compatible con las direcciones IPv6.
6. En la sección **FCoE**:
   a. Seleccione la casilla de verificación **Incluir identidad de FCoE** para incluir identidades de FCoE.
   b. Ingrese una dirección MAC de inicio y especifique la cantidad de identidades de FCoE que se debe crear.

   NOTA: Las direcciones WWPN y WWNN se generan si se agregan los prefijos 0x2001 y 0x2000, respectivamente, a las direcciones MAC.
7. En la sección **Fibre Channel**:
   a. Seleccione la casilla de verificación **Incluir identidad de FC** para incluir identidades de FC.
   b. Ingrese los octetos (seis octetos) del sufijo y la cantidad de direcciones WWPN y WWNN que se debe crear.

   NOTA: Las direcciones WWPN y WWNN se generan si se agrega el prefijo del sufijo proporcionado con 0x2001 y 0x2000, respectivamente.

El grupo de identidades se crea y aparece en la pestaña **Grupos de identidades**.

Crear grupo de identidades: Fibre Channel

Puede agregar direcciones de Fibre Channel (FC) al grupo de identidades. FC se compone de direcciones WWPN/WWNN.

Incluir identidad de FC	Seleccione la casilla para agregar direcciones de FC al grupo de identidades.
Reparación post (6 octetos)	Ingrese la reparación post en uno de los siguientes formatos: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF`

	La longitud de la reparación post puede tener un máximo de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir identidad FC**.
Número de direcciones de WWNN/WWPN	Seleccione el número de dirección de WWPN o WWNN. La dirección puede estar entre 1 y 5000. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir identidad FC**.

Acciones

Anterior	Muestra la ficha **FCoE**.
Finalizar	Guarda los cambios y muestra la página **Configuración**.
Cancelar	Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Crear grupo de identidades: iSCSI

Puede configurar el número de direcciones MAC de iSCSI necesario en la ficha iSCSI.

NOTA: Los atributos iSCSI se aplican únicamente cuando está deshabilitada la opción DHCP para el iniciador de iSCSI en la plantilla de origen.

Incluir direcciones MAC virtuales de iSCSI	Seleccione la casilla para agregar direcciones MAC de iSCSI al grupo de identidades.
Dirección MAC virtual de inicio	Ingrese la dirección MAC de inicio del grupo de identidades en uno de los siguientes formatos: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` La longitud máxima de una dirección MAC es de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.
Número de direcciones MAC de iSCSI	Ingrese el número de direcciones MAC de iSCSI. La dirección MAC puede estar entre 1 y 5000. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.
Configurar el iniciador de iSCSI	Seleccione esta casilla de verificación para configurar el iniciador de iSCSI. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.
Prefijo IQN	Ingrese el prefijo IQN del grupo de identidades de iSCSI. La longitud del prefijo IQN es de un máximo de 200 caracteres. El sistema genera automáticamente el grupo de direcciones de IQN mediante la adición del número generado para el prefijo. Por ejemplo: `<IQN Prefix>.<number>` Esta opción se muestra únicamente si se selecciona la casilla de verificación **Configurar el iniciador de iSCSI**. **NOTA:** El IQN configurado con grupos de identidades no se implementa en el sistema de destino si el modo de arranque es "BIOS". **NOTA:** Si el nombre del iniciador iSCSI se muestra en una línea separada en el campo **Grupos de identidad** > **Uso** > **IQN de iSCSI**, indica que el IQN de iSCSI está activado solo en esa partición de NIC.
Active el grupo de IP del iniciador de iSCSI	Seleccione la casilla de verificación para configurar un grupo de identidades del iniciador de iSCSI. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.
Rango de dirección IP	Ingrese el rango de dirección IP para el grupo del iniciador de iSCSI en uno de los siguientes formatos: • `A.B.C.D - W.X.Y.Z` • `A.B.C.D/E`

Máscara de subred	Seleccione la dirección de máscara de subred del grupo de iSCSI en el menú desplegable.
Puerta de enlace	Ingrese la dirección de la puerta de enlace del grupo de iSCSI.
Primary DNS Server	Ingrese la dirección del servidor DNS principal.
Secondary DNS Server	Ingrese la dirección del servidor DNS secundario.

NOTA: El **Rango de dirección IP**, la **puerta de enlace**, el **Servidor DNS principal** y el **Servidor DNS secundario** deben ser direcciones IPv4 válidas.

Acciones

Anterior	Muestra la ficha **Ethernet**.
Siguiente	Muestra la ficha **FCoE**.
Finalizar	Guarda los cambios y muestra la página **Configuración**.
Cancelar	Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Crear grupo de identidades: Fibre Channel por Ethernet

Puede agregar el número necesario de direcciones MAC de protocolo de inicialización (FIP) de Fibre Channel por Ethernet (FCoE) al grupo de identidades. Los valores de nombre de puerto mundial (WWPN)/nombre de nodo mundial (WWNN) se generan a partir de estas direcciones MAC.

Incluir identidad de FCoE	Seleccione la casilla para incluir las direcciones MAC de FCoE en el grupo de identidades.
Dirección MAC del protocolo FIP	Ingrese la dirección MAC de inicio de protocolo de inicialización FCoE (FIP) del grupo de identidades en uno de los siguientes formatos: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` La longitud máxima de una dirección MAC es de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir identidad FCoE**. Los valores WWPN/WWNN se generan desde la dirección MAC.
Número de identidades FCoE	Seleccione el número necesario de identidades FCoE. Las identidades pueden estar entre 1 y 5000.

Acciones

Anterior	Muestra la ficha **iSCSI**.
Siguiente	Muestra la ficha **Fibre Channel**.
Finalizar	Guarda los cambios y muestra la página **Grupos de identidades**.
Cancelar	Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Crear grupo de identidades: Ethernet

En la ficha **Ethernet**, puede agregar el número de direcciones MAC necesario al grupo de identidades.

Incluir direcciones virtuales Ethernet	Seleccione la casilla para agregar direcciones MAC virtuales al grupo de identidades.
Dirección MAC virtual de inicio	Ingrese la dirección MAC virtual de inicio en uno de los siguientes formatos: • `AA:BB:CC:DD:EE:FF` • `AA-BB-CC-DD-EE-FF` • `AABB.CCDD.EEFF` La longitud máxima de una dirección MAC es de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC virtuales de Ethernet**.
Número de identidades MAC virtuales	Seleccione el número de identidades MAC virtuales. Las identidades pueden ser de 1 a 50. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC virtuales de Ethernet**.

Acciones

Anterior	Muestra la ficha **Información del grupo**.
Siguiente	Muestra la ficha **iSCSI**.
Finalizar	Guarda los cambios y muestra la página **Grupos de identidades**.
Cancelar	Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Ver las definiciones de los grupos de identidades

Para ver las definiciones de un grupo de identidades:

1. En la página **Configuración**, haga clic en **Grupos de identidades**.
2. Seleccione un grupo de identidades y, a continuación, haga clic en **Resumen**.
   Se indican las diversas definiciones de identidades del grupo de identidades.
3. Para ver el uso de las definiciones de estas identidades, haga clic en la pestaña **Uso** y seleccione la opción de filtro **Ver por**.

Editar grupos de identidades

Puede editar un grupo de identidades para agregar rangos que no había especificado anteriormente, agregar un tipo de identidad o eliminar los rangos del tipo de identidad.

Para editar las definiciones de un grupo de identidades:

1. En la página **Configuración**, haga clic en **Grupos de identidades**.
2. Seleccione un grupo de identidades y, a continuación, haga clic en **Editar**.
   Se muestra el cuadro de diálogo **Editar grupo de identidades**.
3. Realice los cambios en las definiciones de las secciones correspondientes y, a continuación, haga clic en **Finalizar**.

Ahora se modificó el grupo de identidades.

Eliminar grupos de identidades

No puede eliminar un grupo de identidades si las identidades están reservadas o asignadas a una plantilla de implementación.

Para eliminar un grupo de identidades:

1. En la página **Configuración**, haga clic en **Grupos de identidades**.
2. Seleccione un grupo de identidades y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Sí**.

Se elimina el grupo de identidades y se eliminan las identidades reservadas asignadas a una o varias plantillas de implementación.

Definir redes

En la página VLAN, puede ingresar información de las redes que están configuradas actualmente en su entorno al que pueden acceder los dispositivos.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Seleccione **Configuración** > **VLAN** > **Definir**.
2. En el cuadro de diálogo **Definir Red**, ingrese un nombre y una descripción adecuada.
3. Ingrese el ID. de VLAN y, a continuación, seleccione el tipo de red.

   Puede seleccionar un tipo de red solamente para el chasis MX7000. Para obtener más información sobre los tipos de red, consulte Tipos de red en la página 100.
4. Haga clic en **Finish** (Finalizar).

La red configurada actualmente en su entorno ahora está definida y los recursos pueden acceder a la red.

NOTA: Las restricciones basadas en el alcance no se aplican a las VLAN, ya que son pools de recursos comunes. Luego de que el administrador define una VLAN, esta queda disponible para que todos los administradores de dispositivos puedan usarla.

Tipos de red

NOTA: Puede seleccionar un tipo de red solo para el chasis MX7000.

Tabla 15. Tipos de red

Tipos de red	Descripción
Propósito general (Bronce)	Se utiliza para tráfico de datos de prioridad baja.
Propósito general (Plata)	Se utiliza para tráfico de datos de prioridad estándar o predeterminada
Propósito general (Oro)	Se utiliza para tráfico de datos de prioridad alta
Propósito general (Platino)	Se utiliza para tráfico de datos de prioridad extremadamente alta
Interconexión de clústeres	Se utiliza para las VLAN de latido del clúster
Gestión del hipervisor	Se utiliza para las conexiones de administración del hipervisor como VLAN de administración de ESXi
Almacenamiento: iSCSI	Se utiliza para las VLAN de iSCSI
Almacenamiento: FCoE	Se utiliza para las VLAN de FCoE
Almacenamiento: replicación de datos	Se utiliza para las VLAN que admiten la replicación de datos de almacenamiento; por ejemplo, para la red de área de almacenamiento virtual de VMware (VSAN)
Migración de máquinas virtuales	Se utiliza para las VLAN que admiten vMotion y tecnologías similares
Registro de VMWare FT	Se utiliza para las VLAN compatibles con la tolerancia a errores VMware

Editar o eliminar una red configurada

1. Vaya a la página de VLAN; para ello, haga clic en **Configuración** > **VLAN**.
2. Seleccione una red de la lista y, a continuación, haga clic en **Editar** en el panel derecho para cambiar el nombre, la descripción, la ID. de VLAN o el tipo de red.

   NOTA: La configuración de VLAN en los chasis M1000e y FX2 no es compatible con una IPv6 infra, ya que el direccionamiento IPv6 no es compatible con el agregador M de E/S (IOA) ni los módulos FN de E/S.

   NOTA: El nombre y los ID de VLAN modificados no se actualizarán en los chasis MX7000 de destino después de ejecutar una tarea de implementación sin estado.

3. Para eliminar la red, seleccione la red y haga clic en **Eliminar**.
4. Haga clic en **Sí**.

Exportar definiciones de VLAN

Las definiciones de red disponibles en OpenManage Enterprise se pueden descargar como un CSV o como un archivo JSON.

1. Para descargar como un archivo CSV:
   a. Haga clic en **Configuración** > **VLAN** > **Exportar** y seleccione **Exportar todo como CSV**.
2. Para descargar como un archivo JSON:
   a. Haga clic en **Configuración** > **VLAN** > **Exportar** y seleccione **Exportar todo como JSON**.

Importar definiciones de red

Las siguientes opciones están disponibles para importar las definiciones de red:

1. **Importar definiciones de VLAN desde un archivo**

   Para importar definiciones de VLAN desde un archivo:

   a. Haga clic en **Configuración** > **VLAN**.
   b. Haga clic en **Importar** y seleccione **Importar desde archivo**.
   c. Vaya hasta la ubicación del archivo y seleccione un archivo .json o .csv existente que contenga las definiciones de VLAN y haga clic en **Abrir**.

   NOTA:

   - Las entradas o el tipo de contenido no válidos en los archivos se marcan y no se importan.
   - Las definiciones de VLAN en los archivos .csv y .json se deben ingresar en los siguientes formatos:

   Tabla 16. Formato de definición VLAN para archivo CSV

Nombre	Descripción	VLANMin	VLANMax	Tipo
VLAN1	VLAN con ID único	1	1	1
VLAN2 (rango)	VLAN con un rango de ID	2	10	2

   y

   Tabla 17. Formato de definición de VLAN para archivos JSON

```
[{"Name":"VLAN1","Description":"VLAN with single ID
","VlanMinimum":1,"VlanMaximum":1,"Type":1},

{"Name":"VLAN2 (Range)","Description":"VLAN with an ID Range
","VlanMinimum":2,"VlanMaximum":10,"Type":2}]
```

d. Haga clic en **Finalizar**. Se crea un trabajo llamado **ImportVLANDefinitionsTask** para importar las redes desde el archivo seleccionado.

2. **Importar definiciones de VLAN desde un chasis**

   Para importar definiciones de VLAN desde un chasis MX7000 existente:

   NOTA: OpenManage Enterprise-Modular versión 1.2 ya debe estar instalado en el MX7000.

   a. Haga clic en **Configuración** > **VLAN**.
   b. Haga clic en **Importar** y seleccione **Importar VLAN desde un chasis**.
   c. En la pantalla **Objetivo del trabajo**, seleccione el chasis desde el que se deben importar las definiciones de VLAN y haga clic en **Aceptar**. Se crea un trabajo con el nombre **ImportVLANDefinitionsTask** para importar las redes desde el chasis seleccionado.

Una vez que finalice el trabajo, actualice la página **Configuración** > **VLAN** para ver las definiciones de VLAN importadas correctamente.

Para ver los detalles de la ejecución del trabajo y el estado de cada red importada desde el chasis, vaya a la página **Trabajos** y haga clic en **Monitorear** > **Trabajos**, seleccione el trabajo y, luego, haga clic en **Ver detalles**.

12

Administrar perfiles

Un “perfil” es una instancia específica de una plantilla de implementación existente que se personaliza con atributos únicos de un dispositivo individual. Los perfiles se pueden crear implícitamente durante la implementación o la implementación automática de una plantilla o a partir de las plantillas existentes por parte del usuario. Un perfil consta de valores de atributos específicos del objetivo junto con las opciones de BootToISO, y detalles de la administración de IP de la iDRAC del dispositivo objetivo. También puede contener cualquier ancho de banda de red y asignaciones de VLAN para los puertos de la NIC del servidor, según corresponda. Los perfiles se vinculan a la plantilla fuente desde la cual se crearon.

En la página **Configuración** > **Perfiles**, se muestran todos los perfiles que están dentro del alcance del usuario que inició sesión. Por ejemplo, un administrador puede ver y administrar todos los perfiles, pero un administrador de dispositivos con alcance limitado solo puede ver y usar los perfiles que haya creado y le pertenezcan.

Se muestran los siguientes detalles de los perfiles enumerados:

Tabla 18. Administrar perfiles: definiciones de campos

Nombre del campo	Descripción
Modificado	Se muestra un símbolo de “modificado” ⚠ para notificar cualquier modificación o cambio en el perfil asociado o en los atributos de la plantilla después de la asignación inicial. Si el perfil modificado se vuelve a implementar en el dispositivo, el símbolo desaparecerá.
Nombre del perfil	Nombre del perfil
Nombre de la plantilla	Nombre de la plantilla fuente vinculada
Destino	Etiqueta de servicio o dirección IP del dispositivo en el que se asignó el perfil. Si el perfil no está asignado a ningún dispositivo, entonces el objetivo está en blanco.
Tipo de destino	El tipo de dispositivo (servidor o chasis) en el que se asignó el perfil.
Chasis	Nombre del chasis si el servidor objetivo se detecta como parte de un chasis.
Estado del perfil	El estado del perfil se mostrará como “Asignado al dispositivo” si el perfil está asignado, “Sin asignar” para los perfiles no asignados e “Implementado” para los perfiles implementados.
Estado de la última acción	Muestra el estado de la última acción del perfil, como anulado, cancelado, completado, fallido, nuevo, no ejecutado, en pausa, en cola, en ejecución, programado, iniciado, detenido, completado con errores.

Los **filtros avanzados** se pueden utilizar para personalizar la lista de perfiles.

En el lado derecho: se muestra la descripción, la hora de la última implementación, la hora de la última modificación, fecha de la creación y el autor de la creación para el perfil seleccionado. Haga clic en Ver identidades para ver la configuración de la NIC y las identidades virtuales que están etiquetadas en el perfil.

Según los distintos estados del perfil, se pueden realizar las siguientes acciones en la página **Configuración** > **Perfiles** como se menciona a continuación:

NOTA: Las operaciones de creación y eliminación no se enumeran como parte de la tabla.

Tabla 19. Estados del perfil y operaciones posibles

Estado del perfil	Editar	Asignar objetivo	Anular asignación del objetivo	Volver a implementar	Migrar
Perfil sin asignar	Sí	Sí	No	No	No
Asignado a dispositivo	Sí	No	Sí	No	No
Implementado	Sí	No	Sí	Sí	Sí

- Cree perfiles y realice una reserva previa de las identidades virtuales. Consulte Crear perfiles en la página 104
- Vea detalles del perfil. Consulte Ver detalles del perfil en la página 105
- Edite ajustes y atributos del perfil. Consulte Editar un perfil en la página 105
- Asigne un perfil a un dispositivo o a una etiqueta de servicio (a través de la implementación automática). Consulte Asignar un perfil en la página 106
- Anule la asignación de un perfil desde un dispositivo o una etiqueta de servicio. Consulte Anular asignación de perfiles en la página 107
- Vuelva a implementar los cambios del perfil en el dispositivo objetivo asociado. Consulte Volver a implementar perfiles en la página 107
- Migre el perfil de un objetivo (dispositivo o etiqueta de servicio) a otro.
- Elimine perfiles. Consulte Eliminar perfiles en la página 108
- Exporte y descargue los perfiles de datos en HTML, CSV o PDF. Consulte Exportar datos de perfiles en formato HTML, CSV o PDF en la página 108

Temas:

Crear perfiles

Los perfiles se pueden crear utilizando las plantillas de implementación existentes para implementarlos en los dispositivos de destino existentes o se pueden reservar para implementarlos de manera automática en los dispositivos que aún no se han detectado.

NOTA:

- Solo los usuarios con privilegios de administrador de dispositivos o de administrador de OpenManage Enterprise pueden realizar las tareas de administración de perfiles. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Después de actualizar a la versión 3.6, todos los perfiles creados por los administradores de dispositivos AD/LDAP y OIDC (PingFederate o KeyCloak) desde cualquiera de las versiones de OpenManage Enterprise anteriores solo se asignan al administrador. Por lo tanto, los administradores de dispositivos deben volver a crear los perfiles después de la actualización.

Para crear un perfil de una plantilla de implementación existente, haga lo siguiente:

1. Vaya a la página Perfiles haciendo clic en **Configuración** > **Perfiles**.
2. Haga clic en **Crear** para activar el asistente para crear perfiles.
3. En la sección Plantilla, seleccione el **Tipo de plantilla** como Servidor o Chasis y, luego, seleccione una plantilla de implementación en la lista desplegable **Seleccionar plantilla**. Haga clic en **Siguiente**.
4. En la página **Detalles**, modifique el **Prefijo del nombre** y proporcione una descripción en el cuadro **Descripción**, si es necesario. En el cuadro **Recuento de perfiles**, ingrese el número de perfiles. Haga clic en **Siguiente**.
5. De manera opcional, en la página **Arrancar desde ISO de red**, seleccione la casilla de verificación **Arrancar desde ISO de red** y especifique la ruta completa de la ISO, la ubicación del recurso compartido de archivos y, luego, seleccione la opción **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo.

6. Haga clic en **Finalizar**.

Los perfiles se crean según el nombre de la plantilla de implementación y el recuento proporcionado. Estos perfiles se muestran en la página Perfiles.

Ver detalles del perfil

Para solo ver los detalles de un perfil existente sin editar:

1. Seleccione un perfil de la lista de perfiles en la página **Configuraciones** > **Perfiles**.
2. Haga clic en **Ver** para activar el asistente para ver el perfil.
3. En la página **Detalles** del asistente, se muestra la información de la plantilla de origen, el nombre, la descripción y el objetivo.
4. Haga clic en **Siguiente**. En la página **Arrancar desde ISO de red**, se muestra la ruta de archivo de imagen ISO, la ubicación compartida del archivo de imagen ISO y el valor del tiempo para adjuntar la ISO si el perfil se estableció inicialmente con esa preferencia.

Perfiles: ver red

Para ver el ancho de banda de red y las asignaciones de VLAN para los puertos de NIC asociados a un perfil:

1. Seleccione un perfil en la página **Configuration** > **perfiles** de configuración.
2. Haga clic en **Ver** para activar el asistente para ver el perfil.
3. La sección **ancho de banda** muestra las siguientes configuraciones de ancho de banda de las NIC particionadas: NIC identificador, puerto, partición, ancho de banda mínimo (%) y ancho de banda máximo (%). Haga clic en **Siguiente**.
4. La sección **VLAN** muestra los siguientes VLAN detalles de los perfiles: NIC formación de equipos, NIC identificador, puerto, equipo, red sin etiqueta y red con etiqueta.
5. Haga clic en **Terminar** para cerrar el asistente.

Editar un perfil

Se puede editar un perfil existente en la página **Configuraciones** > **Perfiles**. Los cambios en el perfil no afectan automáticamente al sistema de destino asociado. Para que los cambios surtan efecto, el perfil modificado debe volver a implementarse en el dispositivo objetivo.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Para cambiar el nombre, editar la red o editar los atributos de un perfil existente, seleccione el perfil en la página Perfiles y haga clic en **Editar**. Se pueden seleccionar las siguientes opciones de edición:

1. Seleccione **Cambiar nombre** y, en el asistente para cambiar el nombre del perfil, edite el nombre del perfil en el cuadro **Nombre**.
2. Seleccione **Editar perfil** para activar el asistente editar el perfil y editar lo siguiente:
   a. En la página **Detalles**, puede editar el **Nombre** y la **Descripción**. Haga clic en **Siguiente**.
   b. En la página Arrancar desde ISO de red, seleccione la casilla de verificación **Arrancar desde ISO de red** para especificar la ruta completa de la ISO y la ubicación del recurso compartido, y realice lo siguiente:
      - Seleccione el **Tipo de recurso compartido** como CIFS o NFS.
      - En el cuadro **Ruta de la ISO**, ingrese la ruta completa de la ISO. Utilice la información sobre herramientas para ingresar la sintaxis correcta.
      - Proporcione los detalles en los cuadros **Dirección IP de recurso compartido**, **Nombre de usuario** y **Contraseña**.
      - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado al dispositivo objetivo. De forma predeterminada, este valor se configura como cuatro horas.
      - Haga clic en **Siguiente**.
   c. En la página **IP de administración de iDRAC**, selecciona una de las siguientes opciones:
      - No cambiar los ajustes de IP.
      - Establecer como DHCP.

- Establecer la IP estática y proporcionar los detalles correspondientes de la IP de administración, la máscara de subred y el gateway.

d. En la página de **Atributos del objetivo**, puede seleccionar y editar los atributos del BIOS, del sistema, de la NIC, de la iDRAC y de la identidad virtual del perfil.
e. Haga clic en **Finalizar** para guardar los cambios.

Asignar un perfil

En la página **Configuración** > **Perfiles**, un perfil sin asignar se puede implementar en un servidor existente o se puede reservar para la implementación automática en un servidor aún por detectar.

NOTA:
- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Los atributos existentes, si los hay, del servidor objetivo se sobrescribirán cuando se implemente un perfil en él.
- Solo los dispositivos que no están asociados con ningún perfil están disponibles para su implementación o una implementación automática.

1. Para **implementar un perfil**:
   a. Seleccione un perfil sin asignar en la página **Configuración** > **Perfiles**, haga clic en **Asignar** > **Implementar** para activar el asistente de implementación de perfiles.
   b. En la página **Detalles**, se muestra la plantilla fuente, el nombre del perfil y la descripción. Haga clic en **Siguiente**.
   c. En la página **Objetivo**:
      - Haga clic en **Seleccionar** y, en la lista de dispositivos, seleccione un dispositivo objetivo.
        NOTA: Los dispositivos que ya tienen asignado un perfil estarán en color gris y no se pueden seleccionar en la lista de destino.
      - Si es necesario reiniciar después de la implementación, seleccione la casilla de verificación **No reiniciar a la fuerza el SO del host si falla el reinicio automático**.
      - Haga clic en **Siguiente**.
   d. (Opcional) En la página **Arrancar desde ISO de red**, seleccione la casilla de verificación **Arrancar desde ISO de red** y proporcione la ruta de la ISO correspondiente, los detalles de la ubicación del recurso compartido y el valor del tiempo para adjuntar la ISO. Haga clic en **Siguiente**.
   e. En la página **IP de administración de iDRAC**, seleccione una de las siguientes opciones y proporcione más detalles importantes.
      - No cambiar la configuración de IP.
      - Establecer como DHCP.
      - Establecer IP estática.
   f. En la página **Atributos de objetivo**, los atributos se muestran en las secciones BIOS, Sistema, NIC y iDRAC. Puede seleccionar, anular la selección o editar los atributos antes de la implementación.
   g. En la página **Identidades virtuales**, haga clic en **Identidades reservadas**. Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
   h. En la página **Programar**, puede elegir **Ejecutar ahora** para implementar el perfil inmediatamente o elegir **Activar programación** y seleccionar una fecha y hora adecuadas para la implementación del perfil.
   i. Haga clic en **Finish** (Finalizar).

   NOTA: Si las identidades ya están asignadas fuera del dispositivo, una implementación nueva no utilizará esas identidades, a menos que se borren. Para obtener más información, consulte Grupos de identidades en la página 95

2. Para **implementar automáticamente un perfil**, siga estos pasos:

   NOTA: En el caso de los dispositivos modulares, la comprobación estricta de las definiciones de VLAN está activada de manera predeterminada.

   a. Seleccione un perfil sin asignar en la página **Configuración** > **Perfiles**, haga clic en **Asignar** > **Implementar automáticamente** para activar el asistente de implementación automática.
   b. En la página Detalles, se muestra la plantilla fuente, el nombre y la descripción (si la hay) del perfil. Haga clic en **Siguiente**.
   c. En la página **Objetivo**, especifique la etiqueta de servicio o el ID del nodo del dispositivo que aún no se ha detectado en el cuadro **Identificador**. Haga clic en **Siguiente**.

d. (Opcional) En la página Arrancar desde ISO de red, seleccione la casilla de verificación **Arrancar desde ISO de red** a fin de especificar la ruta completa de la ISO y la ubicación del recurso compartido.
   - Seleccione el **Tipo de recurso compartido** como CIFS o NFS.
   - En el cuadro **Ruta de la ISO**, ingrese la ruta completa de la ISO. Utilice la información sobre herramientas para ingresar la sintaxis correcta.
   - Proporcione los detalles en los cuadros **Dirección IP de recurso compartido**, **Nombre de usuario** y **Contraseña**.
   - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.

e. Haga clic en **Finish** (Finalizar).

Anular asignación de perfiles

Al utilizar **Configuración** > **Perfiles** > **Anular asignación**, los perfiles implementados o implementados automáticamente se pueden desasociar de sus respectivos objetivos. .

Para anular la asignación de perfiles:

1. Seleccione los perfiles de la lista de perfiles en la página **Configuración** > **Perfil**.
2. Haga clic en **Anular asignación**.
3. Haga clic en **Finalizar** en el cuadro de diálogo de confirmación.

Se anula la asignación de los perfiles seleccionados y se eliminan las identidades de sus respectivos objetivos.

NOTA: En el caso de los dispositivos objetivo implementados, la anulación de la asignación de los perfiles los revertirá a sus identidades asignadas de fábrica.

Volver a implementar perfiles

Para que los cambios en los atributos de un perfil ya implementado surtan efecto en el dispositivo objetivo asociado, se deben volver a implementar. En el caso de los dispositivos modulares, las definiciones de VLAN pueden configurarse durante la reimplementación; sin embargo, la comprobación estricta para que coincida con los atributos de VLAN está deshabilitada.

Para volver a implementar los perfiles, siga estos pasos:

1. En la página **Configuración** > **Perfiles** seleccione los perfiles que tengan el estado “Implementado” o “Modificado” ( ) y haga clic en **Volver a implementar**.
2. En la página Opciones de implementación del atributo del Asistente de reimplementación, seleccione una de las siguientes opciones de implementación de atributos y haga clic en **Siguiente**.
   - **Solo atributos modificados**: se utiliza para volver a implementar solo los atributos modificados en el dispositivo objetivo.
   - **Todos los atributos**: se utiliza para volver a implementar todos los atributos, junto con cualquier atributo modificado, en el dispositivo objetivo.
3. En la página Programar, seleccione una de las siguientes opciones:
   - **Ejecutar ahora** para implementar los cambios de inmediato.
   - **Activar programación** y seleccione una fecha y hora para programar la reimplementación.
4. Haga clic en **Finalizar** para continuar.

Cuando se vuelve a implementar un perfil, se ejecuta un trabajo de **Reimplementación de perfiles**. Puede ver el estado del trabajo en la página **Monitorear** > **Trabajos**.

Migrar un perfil

Un perfil implementado o autoimplementado se puede migrar de la etiqueta de servicio o el dispositivo objetivo existente a otro dispositivo objetivo o etiqueta de servicio idéntico.

Cuando una migración se realiza correctamente, la asignación objetivo del perfil refleja el nuevo objetivo. Si la migración se realiza desde un dispositivo objetivo a una etiqueta de servicio que aún no se ve, el estado del perfil se cambia a “Asignado”.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Migrar perfil cambiará la configuración definida por el perfil (incluidas las identidades virtuales implementadas) de la fuente al objetivo.
- Puede forzar la migración de un perfil incluso si no se puede establecer una conexión con el dispositivo fuente. En este caso, el usuario debe asegurarse de que no existan conflictos de identidad virtual.
- Los atributos específicos del objetivo verdadero no se reciben del servidor "fuente" como parte de la migración. Debido a esto, los mismos detalles de inventario pueden estar presente en dos servidores después de la migración.

Para migrar un perfil, siga estos pasos:

1. En la página **Configuración** > **Perfiles**, seleccione un perfil y haga clic en **Migrar** para activar el asistente de migración de perfiles.
2. En la página Selección:
   a. En el menú desplegable **Seleccionar perfil fuente**, seleccione el perfil que desea migrar.
   b. Haga clic en **Seleccionar objetivo** y, en el cuadro de diálogo Objetivo del trabajo, seleccione un dispositivo objetivo y haga clic en **Aceptar**.
   c. Si es necesario, seleccione la casilla de verificación "Forzar la migración incluso si no se puede establecer una conexión con el dispositivo fuente".

      NOTA: Debe asegurarse de que no existan conflictos de identidad virtual.

   d. Haga clic en **Siguiente**.
3. En la página Programar, seleccione una de las siguientes opciones:
   a. Seleccione **Actualizar ahora** para migrar la configuración del perfil inmediatamente al objetivo.
   b. Seleccione una **fecha** y una **hora** para programar la migración.
4. Haga clic en **Finalizar**.

Se crea un trabajo para migrar la configuración del perfil al nuevo dispositivo objetivo. Puede ver el estado del trabajo en la página **Monitorear** > **Trabajos**.

Eliminar perfiles

Los perfiles "sin asignación" existentes se pueden eliminar de la página **Configuración** > **Perfiles**:

NOTA:

- Un perfil asignado o implementado solo se puede eliminar del portal de perfiles si no está asignado.
- La eliminación de un perfil no asignado con identidades reservadas devuelve esas identidades al grupo de identidades desde el cual provienen. Se recomienda esperar 10 minutos para usar estas identidades recuperadas para reservas e implementaciones futuras.

Para eliminar los perfiles sin asignación:

1. Seleccione los perfiles sin asignar en la página Perfiles.
2. Haga clic en **Eliminar** y confirme haciendo clic en **Sí** cuando se le solicite.

Exportar datos de perfiles en formato HTML, CSV o PDF

Siga estos pasos para exportar datos de perfiles como archivos HTML, CSV o PDF.

1. En la página **Configuración** > **Perfiles** seleccione los perfiles.
2. Haga clic en **Exportar** y, en el cuadro de diálogo Exportar seleccionado, elija una opción (HTML, CSV o PDF).
3. Haga clic en **Finalizar**. Se descargarán los datos de perfiles en el formato seleccionado.

13

Administración del cumplimiento de la configuración del dispositivo

Seleccione **OpenManage Enterprise** > **Configuración** > **Cumplimiento de la configuración** para crear líneas base de configuración-cumplimiento con las plantillas de cumplimiento integradas o creadas por el usuario. Puede crear una plantilla de cumplimiento a partir de una plantilla de implementación existente, un dispositivo de referencia o mediante la importación desde un archivo. Para usar esta función, debe tener la licencia de nivel Enterprise de OpenManage Enterprise e iDRAC para los servidores. Para el controlador de administración del chasis no se requiere licencia. Solo los usuarios que tienen ciertos privilegios pueden utilizar esta característica. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Después de que se crea una línea base de configuración utilizando una plantilla de cumplimiento, el resumen del nivel de cumplimiento de cada línea base se muestra en una tabla. Cada dispositivo asociado a la línea base tiene su propio estado; sin embargo, el estado de máxima gravedad se considera como el estado de la línea base. Para obtener más información sobre el estado de Resumen de condición, consulte el informe técnico *ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.a GENERACIÓN Y POSTERIORES* en el sitio de soporte.

NOTA: En ocasiones, una línea de base con varios dispositivos puede mostrarse como no compatible de forma permanente, debido a que algunos de los valores de atributo no son necesariamente los mismos en todos los destinos. Por ejemplo, los atributos de Control de arranque, como el IQN de destino de iSCSI, la ID de LUN, la WWPN de destino de FCoE, etc., pueden no son iguales en todos los destinos y pueden causar un incumplimiento permanente de la línea de base.

El informe de Resumen general de cumplimiento muestra los campos siguientes:

- **CUMPLIMIENTO**: El nivel de cumplimiento de resumen de dispositivos conectados a una línea base de cumplimiento de configuración. El estado del dispositivo con menor cumplimiento (por ejemplo, crítico) se indica como el estado de toda la línea base.
- **NOMBRE**: El nombre de la línea base de cumplimiento de configuración.
- **PLANTILLA**: nombre de la plantilla de cumplimiento que utiliza la línea base.
- **HORA DE LA ÚLTIMA EJECUCIÓN**: La fecha y la hora más recientes en la que se ejecutó la línea de base de cumplimiento.

Para ver el informe de cumplimiento de configuración de una línea base, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Ver informe** en el panel derecho.

Utilice la característica del generador de consultas para generar el nivel del dispositivo en cuanto al cumplimiento de la línea base seleccionada. Consulte Seleccionar los criterios de una consulta en la página 57.

OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos supervisados y su cumplimiento con la línea base de cumplimiento de configuración. Seleccione **OpenManage Enterprise** > **Monitorear** > **Informes** > **Dispositivos por base de línea de cumplimiento de plantilla** y, luego, haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

Tareas relacionadas

Crear la línea base de cumplimiento de una configuración en la página 112
Editar una línea base de cumplimiento de configuración en la página 113
Eliminar una línea base de cumplimiento de configuración en la página 115
Administrar plantillas de cumplimiento en la página 110
Seleccionar los criterios de una consulta en la página 57

Temas:

Administrar plantillas de cumplimiento

Utilice la plantilla de cumplimiento para crear líneas de base de cumplimiento y, luego, compruebe periódicamente el estado de cumplimiento de configuración de los dispositivos asociados con la línea de base. Consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

Puede crear plantillas de cumplimiento utilizando una plantilla de implementación, un dispositivo de referencia o mediante la importación desde un archivo. Consulte Administrar plantillas de cumplimiento en la página 110.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Cuando selecciona **Configuración** > **Cumplimiento de la configuración** > **Administración de plantillas**, puede ver la lista de plantillas de cumplimiento según el acceso basado en el alcance que tenga en OpenManage Enterprise. Por ejemplo, el administrador puede ver y administrar todas las plantillas de cumplimiento, mientras que el administrador de dispositivos solo puede ver y administrar las plantillas que haya creado y le pertenezcan. En esta página:

- Puede crear una plantilla de cumplimiento:
  - Mediante una plantilla de implementación. Consulte Crear una plantilla de cumplimiento a partir de una plantilla de implementación en la página 110.
  - Mediante un dispositivo de referencia. Consulte Crear una plantilla de cumplimiento a partir de un dispositivo de referencia en la página 111.
  - Mediante la importación desde un archivo de plantilla. Consulte Crear una plantilla de cumplimiento mediante la importación desde un archivo en la página 111.
- Editar una plantilla de cumplimiento. Consulte Editar una plantilla de cumplimiento en la página 112.
- Clonar una plantilla de cumplimiento. Consulte Clonar una plantilla de cumplimiento en la página 111.
- Exportar un informe sobre una plantilla de cumplimiento. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Exportar**. Consulte Exportar todos los datos o aquellos seleccionados en la página 66.
- Eliminar una plantilla de cumplimiento. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Eliminar**.

El cumplimiento de configuración es escalable hasta un máximo de 6000 dispositivos. Para administrar eficientemente la actividad de cumplimiento de configuración a gran escala, realice lo siguiente:

- Deshabilite la tarea de inventario de configuración predeterminada que se activa de forma automática y ejecútela manualmente cuando sea necesario.
- Cree líneas de base de cumplimiento con una menor cantidad de dispositivos. Por ejemplo, los 6000 dispositivos deben categorizarse en cuatro líneas de base independientes con 1500 dispositivos cada una.
- No se debe verificar el cumplimiento de todas las líneas de base al mismo tiempo.

NOTA: Cuando edita una plantilla de cumplimiento, el cumplimiento de configuración se activa automáticamente en todas las líneas de base con las que está asociada. Si existe un caso de uso de edición frecuente de plantillas, el entorno de escalación anterior no es compatible y se recomienda asociar un máximo de 100 dispositivos por línea de base para obtener un rendimiento óptimo.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo en la página 109
Editar una línea base de cumplimiento de configuración en la página 113
Eliminar una línea base de cumplimiento de configuración en la página 115
Crear una plantilla de cumplimiento a partir de una plantilla de implementación en la página 110
Editar una plantilla de cumplimiento en la página 112

Crear una plantilla de cumplimiento a partir de una plantilla de implementación

1. Haga clic en **Configuración** > **Cumplimiento de la configuración** > **Administración de plantillas** > **Crear** > **Desde la plantilla de implementación**.
2. En el cuadro de diálogo **Clonar plantilla de implementación**, en el menú desplegable **Plantilla**, seleccione una plantilla de implementación que se debe utilizar como la referencia para la nueva plantilla.
3. Ingrese un nombre y una descripción para la plantilla de cumplimiento.
4. Haga clic en **Finalizar**.
   Se creará una plantilla de cumplimiento y aparecerá en la lista de plantillas de cumplimiento.

Tareas relacionadas

Administrar plantillas de cumplimiento en la página 110
Clonar una plantilla de cumplimiento en la página 111

Crear una plantilla de cumplimiento a partir de un dispositivo de referencia

Para utilizar las propiedades de configuración de un dispositivo como plantilla para crear una línea de base de configuración, el dispositivo ya debe estar incorporado. Consulte Incorporación de dispositivos en la página 44.

1. Haga clic en **Configuración** > **Cumplimiento de la configuración** > **Administración de plantillas** > **Crear** > **A partir del dispositivo de referencia**.
2. En el cuadro de diálogo **Crear plantilla de cumplimiento**, ingrese un nombre y una descripción para la plantilla de cumplimiento.
3. Seleccione las opciones para crear la plantilla de cumplimiento clonando las propiedades de un servidor o de un chasis.
4. Haga clic en **Siguiente**.
5. En la sección **Dispositivo de referencia**, seleccione el dispositivo que se debe utilizar como "referencia" para crear la plantilla de cumplimiento. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.
   a. Si selecciona un servidor como referencia, seleccione las propiedades de configuración del servidor que se deben clonar.
6. Haga clic en **Finalizar**.
   Un trabajo de creación de plantilla se crea y se ejecuta. La plantilla de cumplimiento recién creada aparece en la página **Plantillas de cumplimiento**.

Crear una plantilla de cumplimiento mediante la importación desde un archivo

1. Haga clic en **Configuración** > **Cumplimiento de la configuración** > **Administración de plantillas** > **Crear** > **Importar desde el archivo**.
2. En el cuadro de diálogo **Importar plantilla de cumplimiento**, ingrese un nombre para la plantilla de cumplimiento.
3. Seleccione el servidor o el tipo de plantilla de chasis y, a continuación, haga clic en **Seleccionar un archivo** para buscar el archivo y seleccionarlo.
4. Haga clic en **Finalizar**.
   Se crea y enumera la plantilla de cumplimiento.

Clonar una plantilla de cumplimiento

1. Haga clic en **Configuración** > **Cumplimiento de la configuración** > **Administración de plantillas**.
2. Seleccione la plantilla de cumplimiento a clonar y, a continuación, haga clic en **Clonar**.
3. En el cuadro de diálogo **Clonar plantilla**, ingrese el nombre de la nueva plantilla de cumplimiento.
4. Haga clic en **Finalizar**.
   De este modo, se crea la nueva plantilla de cumplimiento y se agrega a **Plantillas de cumplimiento**.

Información relacionada

Crear una plantilla de cumplimiento a partir de una plantilla de implementación en la página 110
Editar una plantilla de cumplimiento en la página 112

Editar una plantilla de cumplimiento

Las plantillas de cumplimiento de normas se pueden editar en la página **Cumplimiento de configuración** > **Plantillas de cumplimiento**.

NOTA:

- La edición de una plantilla de cumplimiento que ya está asociada a otras líneas de base generará automáticamente un cumplimiento de configuración para todos los dispositivos en todas las líneas de base que utilizan la plantilla.
- La edición de una plantilla de cumplimiento que está vinculada a varias líneas de base con una gran cantidad de dispositivos puede dar lugar a un cierre de sesión por tiempo de espera agotado, ya que la comprobación de cumplimiento de configuración para todos los dispositivos asociados puede tardar varios minutos. Un tiempo de espera agotado de sesión no indica que los cambios realizados en la plantilla de cumplimiento hayan tenido algún problema.
- Cuando edite una plantilla de cumplimiento en sistemas a gran escala que consten de 1000 dispositivos administrados o un inventario de configuración de un máximo de 6000 dispositivos administrados, asegúrese de que no haya otras operaciones de cumplimiento o inventario de configuración que se ejecuten al mismo tiempo. Además, **deshabilite** el trabajo de inventario de configuración predeterminado generado por el sistema en la página **Monitorear** > **trabajos** (establecer fuente como Generada por el sistema).
- Se recomienda que asocie un máximo de 1500 dispositivos por línea de base para obtener un rendimiento óptimo.
- Si existe un caso de uso de edición frecuente de plantillas, se recomienda asociar un máximo de 100 dispositivos por línea de base para obtener un rendimiento óptimo.

1. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Editar**.
2. En la página **Detalles de la plantilla**, se indican las propiedades de configuración de la plantilla de cumplimiento.
3. Expanda la propiedad que desea editar y, a continuación, ingrese o seleccione datos en los campos.
   a. Para activar la propiedad, seleccione la casilla de verificación, si no está activada.
4. Haga clic en **Guardar** o **Descartar** para implementar o rechazar los cambios.
   La plantilla de cumplimiento queda editada y la información actualizada se guarda.

Tareas relacionadas

Administrar plantillas de cumplimiento en la página 110
Clonar una plantilla de cumplimiento en la página 111

Crear la línea base de cumplimiento de una configuración

Una línea de base de cumplimiento de configuración es una lista de dispositivos asociados a una plantilla de cumplimiento. Un dispositivo en OpenManage Enterprise puede asignarse a 10 líneas de base. Puede comprobar el cumplimiento de un máximo de 250 dispositivos a la vez. .

Para ver la lista de base, haga clic en **OpenManage Enterprise** > **Configuración** > **Cumplimiento de la configuración**.

La lista de líneas de base de cumplimiento disponible depende de su función y sus privilegios de acceso basados en el alcance en OpenManage Enterprise. Por ejemplo, un administrador puede ver y administrar todas las líneas de base de cumplimiento, mientras que un administrador de dispositivos solo puede ver y administrar las líneas de base de cumplimiento que haya creado y le pertenezcan. Además, los dispositivos objetivo disponibles para los administradores de dispositivos están restringidos a los dispositivos o grupos de dispositivos que se encuentran dentro de su alcance respectivo.

Puede crear una línea base de cumplimiento de configuración mediante:

- El uso de una plantilla de implementación existente. Consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.
- El uso de una plantilla capturada de un dispositivo de soporte. Consulte Crear una plantilla de cumplimiento a partir de un dispositivo de referencia en la página 111.
- El uso de una plantilla importada desde un archivo. Consulte Crear una plantilla de cumplimiento mediante la importación desde un archivo en la página 111.

Cuando selecciona una plantilla para la creación de una línea base, también se seleccionan los atributos asociados con las plantillas. Sin embargo, puede editar las propiedades de la línea base. Consulte Editar una línea base de cumplimiento de configuración en la página 113.

PRECAUCIÓN: Si la plantilla de cumplimiento que se utiliza para una línea base ya está asociada con otra línea base, la edición de las propiedades de la plantilla cambia los niveles de cumplimiento de la línea base de los dispositivos ya asociados. Lea el mensaje de error y sucesos que aparece y lleve a cabo las acciones necesarias. Para obtener más información sobre los mensajes de error y sucesos, consulte la *Guía de referencia de mensajes de error y eventos* que se encuentra disponible en el sitio de asistencia.

NOTA: Antes de crear la línea base de cumplimiento de la configuración, asegúrese de que haya creado la plantilla adecuada de cumplimiento.

1. Seleccione **Configuración** > **Cumplimiento de la configuración** > **Crear base**.
2. En el cuadro de diálogo **Crear línea base de cumplimiento**:
   - En la sección **Información de línea base**:
   a. En el menú desplegable **Plantilla**, seleccione una plantilla de cumplimiento. Para obtener más información sobre las plantillas, consulteAdministración del cumplimiento de la configuración del dispositivo en la página 109.
   b. Ingrese un nombre y una descripción para la línea base de cumplimiento.
   c. Haga clic en **Siguiente**.
   - En la sección **Destino**:
   a. Seleccione los dispositivos o grupos de dispositivos. Solo se muestran los dispositivos compatibles. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.

   NOTA: Solo se muestran los dispositivos compatibles. Si selecciona un grupo, los dispositivos que no son compatibles con la plantilla de cumplimiento o los dispositivos que no admiten la función de línea base de cumplimiento de configuración se identifican exclusivamente para ayudarlo a realizar la selección de manera eficaz.

3. Haga clic en **Finish** (Finalizar).
   Se crea y enumera una línea base de cumplimiento. Se inicia una comparación de cumplimiento cuando se crea o se actualiza la línea base. El nivel de cumplimiento general de la línea base se indica en la columna **CUMPLIMIENTO**. Para obtener más información sobre los campos en la lista, consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

   NOTA: Siempre que se crea una línea de base de configuración, el dispositivo crea y ejecuta automáticamente un trabajo de inventario de configuración para recopilar el inventario de los dispositivos asociados con la línea de base, ya que sus datos de inventario no están disponibles. Este trabajo de Inventario de configuración recién creado tiene el mismo nombre que la línea base para la cual se recopila el inventario. Además, en la página Cumplimiento de normas en configuración, se muestra una barra de progreso que indica el progreso del trabajo de inventario junto con la línea de base respectiva.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo en la página 109
Eliminar una línea base de cumplimiento de configuración en la página 115

Editar una línea base de cumplimiento de configuración

Puede editar los dispositivos, el nombre y otras propiedades asociadas con una línea base de configuración. Para ver las descripciones de los campos que aparecen en la lista, consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

PRECAUCIÓN: Si la plantilla de cumplimiento que se utiliza para una línea base ya está asociada con otra línea base, la edición de las propiedades de la plantilla cambia los niveles de cumplimiento de la línea base de los dispositivos ya asociados. Consulte Editar una plantilla de cumplimiento en la página 112. Lea el mensaje de error y sucesos que aparece y lleve a cabo las acciones necesarias. Para obtener más información sobre los mensajes de error y sucesos, consulte la *Guía de referencia de mensajes de error y eventos* que se encuentra disponible en el sitio de asistencia.

1. Seleccione **Configuración** > **Cumplimiento de la configuración**.
2. En la lista de líneas base de cumplimiento de la configuración, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Editar la línea base de cumplimiento**, actualice la información. Consulte Crear la línea base de cumplimiento de una configuración en la página 112.

   NOTA: Siempre que se edita una línea de base de configuración, se activa automáticamente un trabajo de inventario de configuración para recopilar el inventario de los dispositivos asociados con la línea de base cuyos datos de inventario no están disponibles. Este trabajo de inventario de configuración recién creado tiene el mismo nombre que la línea base para la cual se

recopila el inventario. Además, en la página Cumplimiento de normas en configuración, se muestra una barra de progreso que indica el progreso del trabajo de inventario junto con la línea de base respectiva.

Tareas relacionadas

Administrar plantillas de cumplimiento en la página 110
Seleccionar los criterios de una consulta en la página 57

Información relacionada

Administración del cumplimiento de la configuración del dispositivo en la página 109
Eliminar una línea base de cumplimiento de configuración en la página 115

Eliminación de las bases de cumplimiento de la configuración

Puede eliminar las bases de cumplimiento de la configuración en la página **Configuración** > **Cumplimiento de la configuración** y desvincular los dispositivos de las bases asociadas.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

Para eliminar las bases de cumplimiento de la configuración, realice lo siguiente:

1. Seleccione las bases entre las que se enumeran en la página Cumplimiento de la configuración.
2. Haga clic en **Eliminar** y, a continuación, en **Sí** en el mensaje de confirmación.

Las bases de configuración eliminadas se quitan de la página Cumplimiento de la configuración.

Actualización de las bases de cumplimiento de la configuración

La comprobación del estado de una base de cumplimiento se activa automáticamente si se realizan cambios en los atributos de la plantilla de referencia de la base o si se produce algún cambio en el inventario de configuración de cualquiera de los dispositivos asociados a la base.

El estado de cumplimiento de una base de cumplimiento de la configuración es un nivel de cumplimiento acumulado de los dispositivos conectados a dicha base de cumplimiento de la configuración. El estado del dispositivo con menor cumplimiento (por ejemplo, crítico) se indica como el estado de toda la línea base.

El resumen del cumplimiento general de todas las bases de la configuración se representa en un gráfico de anillos ubicado encima de la cuadrícula de la base. La fecha y la hora de la última ejecución de cumplimiento se muestran debajo del gráfico.

La comprobación del estado del cumplimiento de bases grandes puede tardar varios minutos; sin embargo, puede hacer clic en **Actualizar cumplimiento** para obtener un resumen general del cumplimiento de los dispositivos según sea necesario mientras se ejecutan los trabajos de cumplimiento de bases grandes.

NOTA: Cuando el cumplimiento de la configuración se encuentra en estado “En ejecución”, no se permite iniciar nuevos trabajos que afecten a las bases, como la edición de una base o una plantilla de cumplimiento.

Para iniciar una actualización del resumen de cumplimiento general de todas las bases, realice lo siguiente:

1. Haga clic en **Configuración** > **Cumplimiento de la configuración** para que se muestre la página Cumplimiento de la configuración.
2. Haga clic en **Actualizar cumplimiento.**

Se inicia el trabajo de actualización de cumplimiento (Resumen de carga de cumplimiento), se muestra el resumen general del cumplimiento en ese momento y se actualiza el Tiempo de la última ejecución de cumplimiento.

Corrección de dispositivos no compatibles

En la página Informe de cumplimiento una línea base, puede corregir los dispositivos que no coinciden con la línea base asociada cambiando los valores de atributos para que coincidan con los atributos de línea base asociados.

La página Informe de cumplimiento muestra los siguientes campos para los dispositivos de destino que están asociados con la línea base de la plantilla de cumplimiento:

- **CUMPLIMIENTO:** el estado del dispositivo con menor nivel de cumplimiento (por ejemplo, crítico) se indica como el estado de toda la línea de base.
- **NOMBRE DE DISPOSITIVO**: el nombre del dispositivo de destino asociado con la línea base.
- **DIRECCIÓN IP**: la dirección IP del dispositivo de destino.
- **TIPO**: tipo de dispositivo de destino asociado.
- **MODELO**: nombre del modelo del dispositivo de destino.
- **ETIQUETA DE SERVICIO**: la etiqueta de servicio del dispositivo de destino.
- **HORA DE LA ÚLTIMA EJECUCIÓN**: La fecha y la hora más recientes en la que se ejecutó la línea de base de cumplimiento.

Puede utilizar los Filtros avanzados para ver rápidamente los dispositivos que no cumplen con las normas. Además, puede usar el soporte de Seleccionar todo y clasificación en los resultados de cumplimiento de la configuración. Para restablecer los filtros, haga clic en **Borrar filtros**.

Para ver los atributos cambiados de un dispositivo de destino que no cumple con las normas, seleccione el dispositivo y haga clic en **Ver informe**. En la tabla **Informe de cumplimiento** del dispositivo de destino correspondiente se enumeran los nombres de atributo con los valores esperados y actuales de los atributos.

Para corregir uno o más dispositivos que no cumple los requisitos:

1. Seleccione **Configuración** > **Cumplimiento de la configuración**.
2. En la lista de las líneas base de cumplimiento de configuración, seleccione la casilla de verificación correspondiente y, luego, haga clic en **Ver informe**.
3. En la lista de dispositivos que no cumplen, seleccione uno o más dispositivos y, luego, haga clic en **Hacer compatible**.
4. Programe los cambios de configuración para que se ejecuten de inmediato o después y, luego, haga clic en **Finalizar**.

   Para aplicar los cambios de configuración después del siguiente reinicio de servidor, puede seleccionar la opción **Aplicar cambios de configuración en los dispositivos en el siguiente reinicio**.

Se ejecuta una nueva tarea de inventario de configuración y el estado de cumplimiento de la línea base se actualiza en la página **Cumplimiento**.

Exportar el informe de línea base de cumplimiento

Puede exportar una lista completa o parcial de los dispositivos asociados con una línea base de plantilla de cumplimiento a un archivo CSV.

En la página Informe de cumplimiento de una línea base de configuración

1. Haga clic en **Exportar todo** para exportar los detalles de todos los dispositivos de la línea base de cumplimiento. o
2. Haga clic en **Exportar seleccionados** después de seleccionar los dispositivos individuales del informe.

Eliminar una línea base de cumplimiento de configuración

Puede eliminar el nivel de cumplimiento de la configuración de los dispositivos asociados con una línea base de configuración. Para ver las descripciones de los campos que aparecen en la lista, consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.

PRECAUCIÓN: Cuando elimina una línea base de cumplimiento o elimina dispositivos de una línea base de cumplimiento:

- **Los datos de cumplimiento de la línea base o de los dispositivos se eliminan de los datos de OpenManage Enterprise.**
- **Si se elimina un dispositivo, su inventario de configuración ya no se recupera, y la información ya recuperada también se elimina, a menos que el inventario esté asociado con un trabajo de inventario.**

Si una plantilla de cumplimiento que se usa como línea base de cumplimiento está asociada a un dispositivo, no es posible eliminarla. En tal caso, se muestran los mensajes correspondientes. Lea el mensaje de error y sucesos que aparece y lleve a cabo las acciones necesarias.

Para obtener más información sobre los mensajes de error y sucesos, consulte la *Guía de referencia de mensajes de error y eventos* que se encuentra disponible en el sitio de asistencia.

1. Haga clic en **Configuración** > **Cumplimiento de la configuración**.
2. En la lista de líneas base de cumplimiento de la configuración, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Eliminar**.
3. Cuando se le pregunte si desea o no eliminar, haga clic en **SÍ**.
   La línea base de cumplimiento se elimina y la tabla de líneas base **Resumen de cumplimiento general** se actualiza.

Tareas relacionadas

Crear la línea base de cumplimiento de una configuración en la página 112
Seleccionar los criterios de una consulta en la página 57
Administrar plantillas de cumplimiento en la página 110
Editar una línea base de cumplimiento de configuración en la página 113

Información relacionada

Administración del cumplimiento de la configuración del dispositivo en la página 109

14

Monitoreo y administración de alertas de dispositivos

Si selecciona **OpenManage Enterprise** > **Alertas**, podrá ver y administrar las alertas que se generan en los dispositivos en el entorno del sistema de administración. En la página Alertas, se muestran las siguientes pestañas:

- **Registro de alertas**: puede ver y administrar todas las alertas generadas en los dispositivos objetivo.
- **Políticas de alerta**: puede crear políticas de alerta para enviar alertas generadas en dispositivos objetivo a destinos como correos electrónicos, dispositivos móviles, servidores de registro del sistema, etc.
- **Definiciones de alerta**: puede ver las alertas que se generan en caso de error o con fines informativos.

NOTA:

- Para administrar y monitorear alertas de dispositivos en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Las políticas de alerta y los registros de alertas se rigen por el acceso basado en el alcance que tiene en OpenManage Enterprise. Por ejemplo, un administrador puede ver y administrar todas las políticas de alerta, mientras que los administradores de dispositivos solo pueden ver y administrar las políticas de alerta que hayan creado y les pertenezcan. Además, los administradores de dispositivos solo pueden ver las alertas de los dispositivos que se encuentran dentro de su alcance.
- Actualmente, OpenManage Enterprise solo recibe las alertas SNMPv1 y SNMPv2 desde los siguientes servidores PowerEdge: MX840c y MX5016s.
- OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos que supervisa OpenManage Enterprise y las alertas generadas para cada dispositivo. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Informes** > **Cuentas de alertas por informe de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139

Conceptos relacionados

Visualización del registro de alertas en la página 117

Temas:

Visualización del registro de alertas

En la página **Registro de alertas**, se muestra la lista los registros de alertas de los eventos que se producen en los dispositivos. En OpenManage Enterprise, haga clic en **Alertas** > **Registro de alertas**. Aparecerá la página **Registro de alertas**.

De manera predeterminada, solo se muestran las alertas no confirmadas. Puede personalizar la lista de alertas utilizando los **Filtros avanzados**, ubicados en la parte superior izquierda de la lista de alertas, o cambiando la **Configuración de visualización de alertas** en la página **Configuración de la aplicación**. Consulte Personalizar la visualización de alertas en la página 165. Puede ver los detalles de las alertas de la siguiente manera:

- **Confirmar**: si la alerta ha sido confirmada, aparece una marca de verificación en **CONFIRMAR**. Haga clic entre el apóstrofo en **CONFIRMAR** para confirmar o anular la confirmación de una alerta.
- **Hora**: la hora en la que se generó la alerta.
- **Nombre de la fuente**: nombre de host del sistema operativo del dispositivo que generó la alerta. Haga clic en el nombre de la fuente para ver y configurar las propiedades del dispositivo.

  NOTA: No se pueden filtrar las alertas basadas en la dirección IP (nombre de origen) si la alerta se genera desde un dispositivo no detectado o en el caso de una alerta interna.
- **Categoría**: la categoría indica el tipo de alerta. Por ejemplo, el estado del sistema y la auditoría.

- **ID de mensaje**: el ID de la alerta generada.
- **Mensaje**: la alerta generada.
- En la casilla de la derecha se proporciona información adicional, como la descripción detallada y la acción recomendada para una alerta seleccionada.

NOTA: En OpenManage Enterprise versión 3.2 y posteriores, se realiza un seguimiento del punto de datos de la **Última actualización realizada por**; sin embargo, no se hacía un seguimiento de esto en las versiones anteriores. Por lo tanto, tenga en cuenta que si el registro de alertas se refina mediante el campo de filtro avanzado del **usuario**, no se mostrarán las alertas confirmadas de las versiones anteriores.

Seleccione una alerta para ver la información adicional, como la descripción detallada y la acción recomendada, en la parte derecha de la página Registro de alertas. También puede realizar las siguientes tareas en la página Registro de alertas:

- Confirmar alertas
- No confirmar alertas
- Ignorar alertas
- Exportar alertas
- Eliminar alertas
- Alertas archivadas

Información relacionada

Monitoreo y administración de alertas de dispositivos en la página 117

Administración de políticas de alerta

Una vez generados los registros de alertas y que se muestren en la página **Registro de alertas**, puede confirmarlos, anular la confirmación de ellos, ignorarlos, exportarlos, eliminarlos y archivarlos.

Confirmar alertas

Después de ver una alerta y entender su contenido, puede confirmar que ha leído el mensaje de alerta. La confirmación de una alerta evita almacenar el mismo evento en el sistema. Por ejemplo, si un dispositivo es ruidoso y genera el mismo evento varias veces, puede evitar que se realicen más registros de la alerta si confirma que está al tanto de los eventos que recibe del dispositivo. Con ello, no se registrarán más eventos del mismo tipo.

Para confirmar una alerta, en la página **Registro de alertas**, seleccione la casilla de verificación correspondiente a la alerta y, luego, haga clic en **Confirmar**.

Una marca de visto aparece en la columna **CONFIRMAR**. Una vez que se confirma una alerta, se rellena el campo **Última actualización realizada por**, ubicado en la sección de detalles de alerta.

No confirmar alertas

Puede quitar la confirmación de los registros de alerta que están confirmados. Quitar la confirmación de una alerta implica que todos los eventos de cualquier dispositivo se registran incluso cuando el mismo evento se presenta de manera frecuente. De forma predeterminada, ninguna alerta tiene confirmaciones.

Para anular la confirmación de alertas, seleccione la casilla de verificación correspondiente a las alertas y, luego, haga clic en el botón **Anular confirmación**. De lo contrario, puede hacer clic en la marca correspondiente a cada alerta para anular la confirmación.

NOTA: El campo **Última actualización realizada por** en la sección de detalles de alerta conservará el nombre del último usuario que confirmó la alerta.

Ignorar alertas

Si se omite una alerta se crea una directiva de alerta que se activa y se descartan todas las apariciones futuras de dicha alerta. Seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **Ignorar**. De este modo, se muestra un mensaje que indica que se está creando un trabajo para omitir la alerta seleccionada. La cantidad total de alertas que se muestran en la fila de encabezado de OpenManage Enterprise disminuye.

Exportar alertas

Puede exportar registros de alerta en formato .csv a un recurso compartido de red o una unidad local del sistema.

Para exportar registro de alertas, en la página **Registro de alertas**, seleccione los registros de alertas que desea exportar y, luego, haga clic en **Exportar** > **Exportar seleccionados**. Puede exportar todos los registros de alertas. Para ello, haga clic en **Exportar** > **Exportar todos.** Los registros de alerta se exportan en formato .csv.

Eliminar alertas

Puede quitar una alerta para eliminar permanentemente la aparición de la alerta de la consola.

Seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **Eliminar**. Aparece un mensaje en que se le solicitará que confirme el proceso de eliminación. Haga clic en **SÍ** para eliminar la alerta. La cantidad total de alertas que se muestran en la fila de encabezado de OpenManage Enterprise disminuye.

Visualizar las alertas archivadas

Se puede generar y ver un máximo de 50.000 alertas en OpenManage Enterprise. Cuando se alcanza el 95 % del límite de 50.000 (47.500), OpenManage Enterprise genera un mensaje interno que indica que cuando la cuenta alcance 50.000, OpenManage Enterprise purgará automáticamente el 10 % (5000) de las alertas archivadas. En la tabla se muestran diferentes escenarios que involucran la purga de alertas.

Tabla 20. Purga de alertas

Flujo de trabajo	Descripción	Resultado
Purgar tarea	Se ejecuta después de 30 minutos en la consola.	Si las alertas alcanzaron su capacidad máxima (es decir, 50.000), verifique y genere los archivos de purga.
Advertencia de purga de alertas	Genera una advertencia de purga de alertas.	Si las alertas superaron más del 95 % (es decir, 475.000), se genera una alerta de purga interna para purgar el 10 % de las alertas.
Purga de alertas	Alertas purgadas desde el registro de alertas.	Si la cantidad de alertas superó más del 100 %, se purgará el 10 % de las alertas antiguas para volver al 90 % (es decir, 45.000).
Descargar purga de alertas	Descargar alertas purgadas.	Los archivos de las últimas cinco alertas purgadas se pueden descargar en Alertas archivadas.

Descargar las alertas archivadas

Las alertas archivadas son el 10 % más antiguo de las alertas (5000) que se purgan cuando las alertas superan las 50.000. Estas 5000 alertas más antiguas se eliminan de la tabla, se almacenan en un archivo .CSV y, luego, se archivan. Para descargar el archivo de alertas archivadas:

1. Haga clic en **Alertas archivadas**.

   En el cuadro de diálogo **Alertas archivadas**, se muestran las últimas cinco alertas purgadas y archivadas. En esta sección, se indican el tamaño, el nombre y la fecha de archivado.

2. Seleccione la casilla de verificación correspondiente al archivo de alertas y haga clic en **Finalizar**. De este modo, se descarga el archivo .CSV en la ubicación seleccionada.

NOTA: Para descargar alertas archivadas, debe tener los privilegios necesarios. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Directivas de alerta

En este tema, se explica el concepto de políticas de alerta y su utilidad. Para obtener instrucciones sobre la creación, edición, activación, desactivación y eliminación de políticas de alerta, consulte *Configuración y administración de políticas de alerta*.

Las políticas de alerta le permiten configurar y enviar alertas específicas para dispositivos o componentes determinados a un destino particular, como correos electrónicos, dispositivos móviles, servidores de registro del sistema, etc. Las alertas lo ayudan a monitorear y administrar los dispositivos de manera eficaz.

Utilice las políticas de alerta para realizar las siguientes funciones:

- Desencadenar acciones automáticamente en función de la entrada de una alerta.
- Enviar una alerta a una dirección de correo electrónico.
- Enviar una alerta a un teléfono mediante un SMS o una notificación.
- Enviar una alerta mediante una captura SNMP.
- Enviar una alerta a un servidor de registro del sistema.
- Realizar acciones de control de alimentación de los dispositivos, como encender o apagar un dispositivo cuando se genera una alerta de una categoría predefinida.
- Ejecutar un script remoto.

Para ver, crear, editar, activar, desactivar y eliminar políticas de alerta, haga clic en **Alertas** > **Políticas de alerta**.

Tareas relacionadas

Configuración y administración de políticas de alerta en la página 120

Configuración y administración de políticas de alerta

En este tema, se ofrecen instrucciones sobre cómo crear, editar, activar, desactivar y eliminar políticas de alerta.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Información relacionada

Directivas de alerta en la página 120
Reenvío de registros de auditoría a servidores remotos de Syslog en la página 122

Crear una política de alerta

Puede crear políticas de alerta y activarlas para que envíen alertas a direcciones de correo electrónico, teléfonos y capturas SNMP, y para que realicen acciones de control de dispositivos, como encender o apagar un dispositivo, realizar un ciclo de energía y apagar un dispositivo correctamente cuando se genere una alerta de una categoría predefinida.

NOTA: Después de actualizar a la versión 3.6, todas las políticas de alerta que crean los administradores de dispositivos desde cualquiera de las versiones anteriores de OpenManage Enterprise se asignan solo al administrador. Por lo tanto, los administradores de dispositivos deben volver a crear las políticas de alerta después de la actualización para continuar recibiendo las alertas.

En la página **Alertas** > **Políticas de alerta**, haga clic en **Crear** y realice lo siguiente:

1. Ingrese un nombre y la descripción para la política de alerta y haga clic en **Siguiente**. La casilla de verificación **Habilitar política** está seleccionada de manera predeterminada.
2. Seleccione la categoría de alerta mediante la elección de una o todas las categorías de base de información de administración (MIB) de otros fabricantes incorporadas e importadas.

   Puede expandir cada categoría para ver y seleccionar las subcategorías. Para obtener más información sobre las categorías y subcategorías, consulte Definiciones de alerta en la página 125.
3. Seleccione los dispositivos o grupos para los que se necesita una alerta y haga clic en **Siguiente**. Se puede aplicar una alerta para lo siguiente:
   - Un dispositivo o varios dispositivos.
   - Un grupo o varios grupos de dispositivos.

- Un dispositivo no detectado específico ingresando su dirección IP o nombre de host.
- Cualquier dispositivo no detectado.

  NOTA: No se pueden realizar las tareas de ejecución de script remoto ni de acción de encendido en los dispositivos no detectados.

  NOTA: En OpenManage Enterprise se reconocen las alertas de SNMPv1, SNMPv2 y los protocolos de SNMPv3 enviados por dichos dispositivos no detectados (externos).

4. (Opcional) Especifique la duración de la aplicación de la política de alertas mediante la selección de los valores necesarios para **Rango de fechas**, **Intervalo de tiempo** y **Días**, y, luego, haga clic en **Siguiente**.
5. Seleccione la gravedad de la alerta y haga clic en **Siguiente**.

   Para seleccionar todas las categorías de gravedad, seleccione la casilla de verificación **Todas**.
6. Seleccione una o más acciones de alerta y haga clic en **Siguiente**. Las opciones disponibles son:
   - Correo electrónico: seleccione Correo electrónico para enviar un correo electrónico a un destinatario designado especificando la información de cada campo y utilizando tokens si es necesario para el asunto y el mensaje. Consulte Sustitución del token en secuencias de comandos remotas y política de alerta en la página 181

     NOTA: Correos electrónicos para varias alertas de la misma categoría, el ID de mensaje y el contenido se activan solo una vez cada dos minutos para evitar mensajes de alerta redundantes o repetidos en la bandeja de entrada.
   - Reenvío de SNMP Trap (Activar): haga clic en Activar para ver la ventana de Configuración de SNMP en la que podrá definir la configuración de SNMP para la alerta. Consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122.
   - Syslog (Activar): haga clic en Activar para ver la ventana de Configuración de Syslog en la que puede definir la configuración del registro del sistema para la alerta. Consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122.
   - Seleccione la casilla de verificación Omitir para omitir un mensaje de alerta y no activar la directiva de alerta.
   - Envíe un SMS al número de teléfono especificado.
   - Control de alimentación: seleccione la casilla de verificación Control de alimentación para ver las acciones en las que puede encender, apagar, realizar un ciclo de energía o apagar correctamente un dispositivo. Para apagar un sistema operativo antes de realizar acciones de control de alimentación, seleccione la casilla de verificación **Primero apagar SO**.
   - Ejecución de script remoto (Activar): haga clic en Activar para ver la ventana Ajustes de comandos remotos en la que puede agregar y ejecutar comandos remotos en nodos remotos. Si desea obtener más información sobre cómo comandos remotos, consulte Ejecutar comandos y scripts remotos en la página 123.

     En el menú desplegable, seleccione el script que desea ejecutar cuando se ejecute esta política de alerta. Puede configurar la ejecución del comando remoto también como se describe en Administración de los ajustes del servidor OpenManage Enterprise en la página 146.
   - Envíe una notificación al teléfono móvil registrado en OpenManage Enterprise. Consulte Configuración de OpenManage Mobile en la página 174.
7. Revise los detalles de la política de alerta creada en la pestaña Resumen y haga clic en **Finalizar**.
   De este modo, se crea correctamente la directiva de alerta y se agrega a la sección **Directivas de alerta**.

Administrar políticas de alerta

Una vez que se hayan creado las políticas de alerta en la página **Políticas de alerta**, podrá editarlas, activarlas, desactivarlas y eliminarlas. Además, OME proporciona políticas de alerta incorporadas que desencadenan acciones asociadas cuando se recibe la alerta. No puede editar ni eliminar las políticas de alerta incorporadas, solo puede activarlas o desactivarlas.

Para ver las políticas de alerta creadas, haga clic en **Alertas** > **Políticas de alerta**.

Para seleccionar todas las políticas de alerta, seleccione la casilla de verificación a la izquierda de **Activada**. Seleccione una o más casillas de verificación junto a la política de alerta para realizar las siguientes acciones:

- **Editar una política de alerta**: seleccione una política de alerta y haga clic en **Editar** para modificar la información necesaria en el cuadro de diálogo Configuración y administración de políticas de alerta en la página 120.

  NOTA: Solo se puede editar una política de alerta a la vez.

  NOTA: La casilla de verificación Intervalo de tiempo está desactivada de manera predeterminada para las políticas de alerta de las versiones de OpenManage Enterprise anteriores a la versión 3.3.1. Después de actualizar, active la opción Intervalo de tiempo y actualice los campos para reactivar las políticas.
- **Activar políticas de alerta**: seleccione la política de alerta y haga clic en **Activar**. Cuando una política de alerta está habilitada, aparece una marca de verificación en la columna **Habilitada**. El botón **Habilitar** de una directiva de alerta que ya esté habilitada se ve atenuado.
- **Desactivar políticas de alerta**: seleccione la política de alerta y haga clic en **Desactivar**. La política de alerta está desactivada y se elimina la marca de verificación en la columna **ACTIVADA**.

También puede desactivar una política de alerta mientras la crea si desmarca la casilla de verificación **Activar política** en la sección Nombre y descripción.

- **Eliminar políticas de alerta**: seleccione la política de alerta y haga clic en **Eliminar**.

  Puede eliminar varias directivas de alerta a la vez mediante la selección de las casillas de verificación correspondientes. Para seleccionar o desmarcar todas las casillas de verificación, seleccione la que se encuentra en la fila de encabezado junto a **HABILITADA**.

Reenvío de registros de auditoría a servidores remotos de Syslog

Para supervisar todos los registros de auditoría de OpenManage Enterprise desde los servidores de Syslog, puede crear una política de alerta. Todos los registros de auditoría, como los intentos de inicio de sesión del usuario, la creación de las políticas de alertas y la ejecución de diversos trabajos pueden reenviarse a los servidores de Syslog.

Para crear una política de alerta a fin de reenviar los registros de auditoría a los servidores de Syslog, realice lo siguiente:

1. Seleccione **Alertas** > **Políticas de alertas** > **Crear**.
2. En el cuadro de diálogo **Crear política de alerta**, en la sección **Nombre y descripción**, ingrese el nombre y la descripción de la política de alerta.
   a. La casilla de verificación **Activar política** está seleccionada de forma predeterminada para indicar que la política de alerta se activará en cuanto se cree. Para deshabilitar la política de alerta, desmarque la casilla de verificación. Para obtener más información sobre la activación de las políticas de alertas en otro momento, consulte Configuración y administración de políticas de alerta en la página 120.
   b. Haga clic en **Siguiente**.
3. En la sección **Categoría**, abra **Aplicación** y seleccione las categorías y las subcategorías de los registros del dispositivo. Haga clic en **Siguiente**.
4. En la sección **Destino**, la opción **Seleccionar dispositivos** está seleccionada de forma predeterminada. Haga clic en **Seleccionar dispositivos** y seleccione los dispositivos del panel izquierdo. Haga clic en **Siguiente**.

   NOTA: La selección de dispositivos o grupos de destino no es posible mientras se reenvían los registros de auditoría al servidor de Syslog.

5. (Opcional) De forma predeterminada, las políticas de alertas siempre están activas. Para limitar la actividad, en la sección **Fecha y hora**, seleccione las fechas de inicio y de término del rango y, luego, seleccione el período.
   a. Seleccione las casillas de verificación correspondientes a los días en los que se deben ejecutar las políticas de alerta.
   b. Haga clic en **Siguiente**.
6. En la sección **Gravedad**, seleccione el nivel de gravedad de las alertas para las cuales se debe activar esta política.
   a. Para seleccionar todas las categorías de gravedad, seleccione la casilla de verificación **Todas**.
   b. Haga clic en **Siguiente**.
7. En la sección **Acciones**, seleccione **Syslog**.

   Si los servidores de Syslog no están configurados en OpenManage Enterprise, haga clic en **Activar** e ingrese la dirección IP de destino o el nombre de host de los servidores de Syslog. Para obtener más información acerca de la configuración de los servidores de Syslog, consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122.
8. Haga clic en **Siguiente**.
9. En la sección **Resumen**, se muestran los detalles de la política de alerta definida. Lea detenidamente la información.
10. Haga clic en **Finalizar**.

De este modo, se crea correctamente la directiva de alerta y se agrega a la sección **Directivas de alerta**.

Tareas relacionadas

Configuración y administración de políticas de alerta en la página 120
Monitoreo de registros de auditoría en la página 126

Configurar alertas de SMTP, SNMP y registro del sistema

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Alertas**, puede configurar la dirección de correo electrónico (SMTP) que recibe las alertas del sistema, los destinos de reenvío de alertas SNMP y las propiedades de reenvío de Syslog. Para administrar estas configuraciones, debe contar con credenciales de nivel de administrador de OpenManage Enterprise.

Para configurar y autenticar el servidor SMTP que administra la comunicación por correo electrónico entre los usuarios y OpenManage Enterprise, haga lo siguiente:

1. Expanda **Configuración de correo electrónico**.
2. Ingrese la dirección de red del servidor SMTP que envía mensajes de correo electrónico.
3. Para autenticar el servidor SMTP, seleccione la casilla de verificación **Activar autenticación** e ingrese el nombre de usuario y la contraseña.
4. De manera predeterminada, el número de puerto SMTP al que se debe acceder es 25. Edite según sea necesario.
5. Seleccione la casilla de verificación **Utilizar SSL** para proteger la transacción SMTP.
6. Para probar si el servidor SMTP funciona correctamente, haga clic en la casilla de verificación **Enviar correo electrónico de prueba** e ingrese un **destinatario de correo electrónico**.
7. Haga clic en **Aplicar**.
8. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para configurar los ajustes de reenvío de alertas SNMP, haga lo siguiente:

1. Expanda **Configuración de reenvío de alertas SNMP**.
2. Seleccione la casilla de verificación **HABILITADA** para habilitar las capturas SNMP respectivas para enviar alertas en caso de sucesos predefinidos.
3. En la casilla **DIRECCIÓN DE DESTINO**, ingrese la dirección IP del dispositivo de destino que debe recibir la alerta.

   NOTA: No se permite ingresar la IP de la consola para evitar la duplicación de alertas.
4. En el menú **VERSIÓN DE SNMP**, seleccione el tipo de versión de SNMP como SNMPv1, SNMPv2 o SNMPv3, y complete los campos a continuación:
   a. En el cuadro CADENA DE COMUNIDAD, ingrese la cadena de comunidad SNMP del dispositivo que debe recibir la alerta.
   b. Edite el NÚMERO DE PUERTO, si es necesario. El número de puerto predeterminado para las capturas SNMP es 162. Consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
   c. Si se selecciona SNMPv3, proporcione los siguientes detalles adicionales:
      i. NOMBRE DE USUARIO: proporcione un nombre de usuario.
      ii. TIPO DE AUTENTICACIÓN: en la lista desplegable, seleccione SHA, MD_5 o Ninguno.
      iii. FRASE DE CONTRASEÑA DE AUTENTICACIÓN: proporcione una frase de contraseña de autenticación con un mínimo de ocho caracteres.
      iv. TIPO DE PRIVACIDAD: en la lista desplegable, seleccione DES, AES_128 o Ninguno.
      v. FRASE DE CONTRASEÑA DE PRIVACIDAD: proporcione una frase de contraseña de privacidad con un mínimo de ocho caracteres.
5. Para probar un mensaje SNMP, haga clic en el botón **Enviar** de la captura correspondiente.
6. Haga clic en **Aplicar**. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para actualizar la configuración de reenvío de registro del sistema, haga lo siguiente:

1. Expanda **Configuración de reenvío de Syslog**.
2. Seleccione la casilla de verificación para habilitar la característica de Syslog en el servidor correspondiente en la columna **SERVIDOR**.
3. En la casilla **DIRECCIÓN/NOMBRE DE HOST DE DESTINO**, ingrese la dirección IP del dispositivo que recibe los mensajes de Syslog.
4. Se accede al número de puerto predeterminado cuando UDP equivale a 514. Ingrese o seleccione en la casilla, si fuera necesario editar. Consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
5. Haga clic en **Aplicar**.
6. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Ejecutar comandos y scripts remotos

Cuando recibe una SNMP trap, puede ejecutar un script en OpenManage Enterprise. Esto establece una política que abre un vale en el sistema de generación de vales de terceros para la administración de alertas. Puede crear y almacenar solo hasta **cuatro** comandos remotos.

NOTA: El uso de los siguientes caracteres especiales como parámetros de la CLI de IPMI y RACADM no es soportado: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * y **'**.

1. Haga clic en **Configuración de la aplicación** > **Ejecución del script**.
2. En la sección **Configuración de comandos remotos**, haga lo siguiente:
   a. Para agregar un comando remoto, haga clic en **Crear**.
   b. En la casilla **Nombre del comando**, escriba el nombre del comando.
   c. Seleccione uno de los siguientes tipos de comando:

i. Script
ii. RACADM
iii. Herramienta IPMI

d. Si selecciona **Script**, haga lo siguiente:
   i. En la casilla **Dirección IP**, ingrese la dirección IP.
   ii. Seleccione el método de autenticación: **contraseña** o **clave SSH**.
   iii. Especifique el **Nombre de usuario** y la **Contraseña** o la **clave SSH**.
   iv. En la casilla **Comando**, escriba los comandos.
      - Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
      - La sustitución de token en secuencias de comandos es posible. Consulte Sustitución del token en secuencias de comandos remotas y política de alerta en la página 181
   v. Haga clic en **Finalizar**.

e. Si selecciona **RACADM**, haga lo siguiente:
   i. En la casilla **Nombre del comando**, escriba el nombre del comando.
   ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
   iii. Haga clic en **Finalizar**.

f. Si selecciona **Herramienta IPMI**, haga lo siguiente:
   i. En la casilla **Nombre del comando**, escriba el nombre del comando.
   ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
   iii. Haga clic en **Finalizar**.

3. Para editar la configuración de los comandos remotos, seleccione el comando y haga clic en **Editar**.
4. Para eliminar la configuración de los comandos remotos, seleccione el comando y haga clic en **Eliminar**.

Actualización automática del chasis MX7000 sobre inserción y eliminación de sleds

OpenManage Enterprise puede reflejar casi instantáneamente la adición o eliminación de sleds después de que un chasis MX7000 independiente o principal se detecta o incorpora.

Cuando se detecta o se incorpora un chasis MX7000 independiente o principal mediante el uso de OpenManage Enterprise (versiones 3.4 y posteriores), se crea simultáneamente una política de alerta en el chasis MX7000. Para obtener más información acerca de la detección y la incorporación de dispositivos en OpenManage Enterprise, consulte Crear un trabajo de detección de dispositivos en la página 43 y Incorporación de dispositivos en la página 44.

La política de alerta creada automáticamente en el dispositivo MX7000 OpenManage Enterprise-Modular activa un trabajo de actualización del inventario de chasis, denominado **Actualizar el inventario del chasis**, en OpenManage Enterprise cada vez que se inserta, elimina o reemplaza un sled en el chasis MX7000.

Una vez que se completa el trabajo de actualización del chasis e inventario, los cambios relacionados con el sled del MX7000 se muestran en la página Todos los dispositivos.

Se deben cumplir los siguientes requisitos durante la incorporación del chasis MX7000 para la creación correcta de la política de alerta automática:

- OpenManage Enterprise-Modular versión 1.2 ya debe estar instalado en el MX7000.
- El chasis MX7000 se debe incorporar con las opciones **"Habilitar recepción de trap de servidores iDRAC y chasis MX7000 detectados"** y **"Establecer cadena de comunidad para el destino trap desde los ajustes de la aplicación"**.
- La IP del dispositivo OpenManage Enterprise se debe registrar de manera correcta como uno de los cuatro destinos de alerta disponibles en el MX7000 recientemente incorporado. Si todos los destinos de alerta en el MX7000 ya están configurados al momento de la incorporación, se producirá un error durante la creación de la política de alerta automática.

NOTA:

- La política de alerta del MX7000 solo es específica para los sleds y no se aplica a los demás componentes del chasis, como los IOM.
- Las preferencias de alerta del MX7000 se pueden establecer en OpenManage Enterprise para recibir todas las alertas o solo las de la categoría de chasis desde el MX7000. Para obtener más información, consulte Administración de preferencias de consola en la página 163.

- Se espera que haya alguna demora entre la acción real de los sleds y la activación de la actualización del inventario de chasis en OpenManage Enterprise.
- La política de alerta creada automáticamente se elimina si el chasis MX7000 se elimina del inventario de dispositivos de OpenManage Enterprise.
- En la página Todos los dispositivos, se mostrará el **Estado administrado** de un chasis MX7000 incorporado correctamente con una política de reenvío de alertas automáticas como "Administrado con alertas". Para obtener más información acerca de la incorporación, consulte Incorporación de dispositivos en la página 44

Definiciones de alerta

Si hace clic en **OpenManage Enterprise** > **Alertas** > **Definiciones de alerta**, puede ver las alertas que se generan en caso de error o con fines informativos. Estos mensajes:

- Se conocen como mensajes de eventos y errores.
- Se muestran en la interfaz gráfica de usuario (GUI) y la interfaz de línea de comandos (CLI) para RACADM y WS-Man.
- Se guardan en los archivos de registro solo con fines informativos.
- Se enumeran y definen claramente para permitir que implemente acciones correctivas y preventivas de forma eficaz.

Un mensaje de error y sucesos tiene:

- **ID DE MENSAJE**: los mensajes se clasifican en función de componentes como BIOS, fuente de energía (PSU), almacenamiento (STR), datos de registro (LOG) y Chassis Management Controller (CMC).
- **MENSAJE**: la causa real de un suceso. Los sucesos solo se desencadenan para fines informativos o cuando hay un error en la realización de tareas.
- **CATEGORÍA**: clase a la que pertenece el mensaje de error. Para obtener más información acerca de las categorías, consulte la *guía de referencia de mensajes de error y sucesos para los servidores Dell EMC PowerEdge* disponible en el sitio de soporte.
- **Acción recomendada**: solución del error mediante los comandos de la GUI, RACADM o WS-Man. En caso de ser necesario, se recomienda consultar los documentos en el sitio de soporte o TechCenter para obtener más información.
- **Descripción detallada**: más información sobre un problema para obtener una solución sencilla y rápida.

Puede ver más información acerca de una alerta utilizando filtros como ID de mensaje, texto del mensaje, categoría y subcategoría. Para ver las definiciones de alerta:

1. En el menú **OpenManage Enterprise**, en **Alertas**, haga clic en **Definiciones de alerta**.

   En **Definiciones de alerta**, aparece una lista de todos los mensajes de alerta estándar.

2. Para buscar un mensaje de error rápidamente, haga clic en **Filtros avanzados**.

En el panel derecho se muestra información sobre los mensajes de error y sucesos de la ID de mensaje que se seleccionó en la tabla.

15

Monitoreo de registros de auditoría

En la página **OpenManage Enterprise** > **Monitorear** > **Registros de auditoría**, se muestran los datos de registro para ayudarlo a usted o a los equipos de soporte de Dell EMC durante el análisis y la solución de problemas. El registro de auditoría se realiza en los siguientes casos:

- Se asignan o cambian los permisos de acceso de un grupo.
- Se modifica el rol de usuario.
- Las acciones realizadas en los dispositivos con monitoreo de OpenManage Enterprise.

Los archivos de registro de auditoría se pueden exportar a formatos de archivo CSV. Consulte Exportar todos los datos o aquellos seleccionados en la página 66.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Las restricciones basadas en el alcance no se aplican a los registros de auditoría.

1. Para ver los registros de auditoría, seleccione **Monitorear** > **Registros de auditoría**.
   Aparecen los registros de auditoría de las tareas realizadas que OpenManage Enterprise almacena y muestra mediante el dispositivo. Por ejemplo, los intentos de inicio de sesión del usuario, la creación de directivas de alerta y la ejecución de diferentes trabajos.
2. Para ordenar los datos en cualquiera de las columnas, haga clic en el título de la columna.
3. Para buscar información rápidamente sobre un registro de auditoría, haga clic en **Filtros avanzados**.
   Los campos que aparecen a continuación funcionan como filtros para buscar datos rápidamente.
4. Ingrese o seleccione datos en los siguientes campos:
   - **Gravedad**: seleccione el nivel de gravedad de los datos de registro. Las opciones disponibles son Información, Advertencia y Crítico.
     - Crítico: se produjo una acción inusual. Se requiere atención inmediata.
     - Advertencia: El evento es importante, pero no requiere atención inmediata.
     - Información: cualquier acción realizada con éxito.
   - **Hora de inicio** y **Hora de finalización**: para ver los registros de auditoría de un período específico.
   - **Usuario**: para ver los registros de auditoría de un usuario específico. Por ejemplo, administrador, sistema, administrador de dispositivos y observador.
   - **Dirección de la fuente**: para ver los registros de auditoría de un sistema específico. Por ejemplo, el sistema en el que haya iniciado la sesión de OpenManage Enterprise.
   - **Categoría**: para ver los registros de auditoría de tipo auditoría o configuración.
     - Auditoría: se genera cuando un usuario inicia sesión o sale del dispositivo OpenManage Enterprise.
     - Configuración: se genera cuando se realiza una acción en un dispositivo de destino.
   - **Descripción contiene**: ingrese el texto o la frase contenidos en los datos de registro que busca. Aparecen todos los registros que contienen el texto seleccionado. Por ejemplo, si ingresa `warningSizeLimit`, se muestran todos los registros con este texto.
   - **ID de mensaje**: ingrese la ID de mensaje. Si los criterios de búsqueda coinciden, solo se muestran los elementos con el ID de mensaje coincidente.
5. Para quitar el filtro, haga clic en **Borrar todos los filtros**.
6. Para exportar uno o todos los registros de auditoría, seleccione **Exportar** > **Exportar seleccionados** o **Exportar** > **Exportar todos** respectivamente. Para obtener más información acerca de la exportación de registros de auditoría, consulte Exportar todos los datos o aquellos seleccionados en la página 66.
7. Para exportar los registros de la consola como un archivo .ZIP, haga clic en **Exportar** > **Exportar registros de la consola**.

NOTA:

- Actualmente, en lo que respecta a todos los chasis M1000e detectados con una versión de firmware de chasis 5.1x y anteriores, la fecha en la columna HORA DE REGISTRO en Registros de hardware se muestra como 12 de ENE del 2013. Sin embargo, en todas las versiones de chasis VRTX y FX2, aparece la fecha correcta.
- El archivo no estará listo de inmediato para su descarga, especialmente en los casos en los que se recopila un gran conjunto de registros. El proceso de recopilación se realiza en segundo plano y, una vez finalizada la operación, se muestra una indicación para guardar el archivo.

Información relacionada

Reenvío de registros de auditoría a servidores remotos de Syslog en la página 122

Temas:

Reenvío de registros de auditoría a servidores remotos de Syslog

Para supervisar todos los registros de auditoría de OpenManage Enterprise desde los servidores de Syslog, puede crear una política de alerta. Todos los registros de auditoría, como los intentos de inicio de sesión del usuario, la creación de las políticas de alertas y la ejecución de diversos trabajos pueden reenviarse a los servidores de Syslog.

Para crear una política de alerta a fin de reenviar los registros de auditoría a los servidores de Syslog, realice lo siguiente:

1. Seleccione **Alertas** > **Políticas de alertas** > **Crear**.
2. En el cuadro de diálogo **Crear política de alerta**, en la sección **Nombre y descripción**, ingrese el nombre y la descripción de la política de alerta.
   a. La casilla de verificación **Activar política** está seleccionada de forma predeterminada para indicar que la política de alerta se activará en cuanto se cree. Para deshabilitar la política de alerta, desmarque la casilla de verificación. Para obtener más información sobre la activación de las políticas de alertas en otro momento, consulte Configuración y administración de políticas de alerta en la página 120.
   b. Haga clic en **Siguiente**.
3. En la sección **Categoría**, abra **Aplicación** y seleccione las categorías y las subcategorías de los registros del dispositivo. Haga clic en **Siguiente**.
4. En la sección **Destino**, la opción **Seleccionar dispositivos** está seleccionada de forma predeterminada. Haga clic en **Seleccionar dispositivos** y seleccione los dispositivos del panel izquierdo. Haga clic en **Siguiente**.

   NOTA: La selección de dispositivos o grupos de destino no es posible mientras se reenvían los registros de auditoría al servidor de Syslog.

5. (Opcional) De forma predeterminada, las políticas de alertas siempre están activas. Para limitar la actividad, en la sección **Fecha y hora**, seleccione las fechas de inicio y de término del rango y, luego, seleccione el período.
   a. Seleccione las casillas de verificación correspondientes a los días en los que se deben ejecutar las políticas de alerta.
   b. Haga clic en **Siguiente**.
6. En la sección **Gravedad**, seleccione el nivel de gravedad de las alertas para las cuales se debe activar esta política.
   a. Para seleccionar todas las categorías de gravedad, seleccione la casilla de verificación **Todas**.
   b. Haga clic en **Siguiente**.
7. En la sección **Acciones**, seleccione **Syslog**.

   Si los servidores de Syslog no están configurados en OpenManage Enterprise, haga clic en **Activar** e ingrese la dirección IP de destino o el nombre de host de los servidores de Syslog. Para obtener más información acerca de la configuración de los servidores de Syslog, consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122.
8. Haga clic en **Siguiente**.
9. En la sección **Resumen**, se muestran los detalles de la política de alerta definida. Lea detenidamente la información.
10. Haga clic en **Finalizar**.

De este modo, se crea correctamente la directiva de alerta y se agrega a la sección **Directivas de alerta**.

Tareas relacionadas

Configuración y administración de políticas de alerta en la página 120
Monitoreo de registros de auditoría en la página 126

16

Utilización de trabajos para el control de dispositivos

Un trabajo es un conjunto de instrucciones para realizar una tarea en uno o más dispositivos. Los trabajos incluyen detección, actualización del firmware, actualización del inventario de dispositivos, garantía, etc. Puede ver el estado y los detalles de los trabajos que se inician en los dispositivos y sus subcomponentes en la página **Trabajos**. OpenManage Enterprise tiene muchos trabajos de mantenimiento internos que se activan en un programa establecido automáticamente por el dispositivo. Para obtener más información sobre los trabajos "predeterminados" y su programa, consulte Programa y trabajos predeterminados de OpenManage Enterprise en la página 130 .

Requisitos previos:

Crear y administrar trabajos, como parpadeo, control de alimentación, administración de bases del firmware, administración de base de cumplimiento de la configuración, etc., en las que está involucrada la tarea de selección de dispositivos.

- Debe tener los privilegios de usuario necesarios. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Cada tipo de trabajo se limita a los dispositivos en los que debe tener lo siguiente:
  - Permisos de acceso.
  - Capacidad de completar la acción necesaria.

Para crear y administrar trabajos, seleccione **OpenManage Enterprise** > **Monitorear** > **Trabajos**. Puede realizar las siguientes tareas en la página **Trabajos**:

- Ver la lista de los trabajos que se están ejecutando actualmente, que han fallado, y que se han completado correctamente.
- Crear trabajos para hacer parpadear los LED del dispositivo, controlar la alimentación del dispositivo y ejecutar un comando remoto en los dispositivos. Consulte Crear un trabajo de comando remoto para la administración de dispositivos en la página 133, Creación de trabajos para administrar dispositivos de alimentación y Creación de un trabajo para hacer parpadear los LED del dispositivo. Puede realizar acciones similares en un servidor desde la página de detalles del dispositivo. Consulte Ver y configurar dispositivos individuales en la página 67.
- Administrar trabajos, como ejecutar, detener, activar, desactivar o eliminar trabajos.

Para ver más información sobre un trabajo, seleccione la casilla de verificación correspondiente a un trabajo y, a continuación, haga clic en **Ver detalles** en el panel derecho. Consulte Visualización de la información de trabajos.

Temas:

Ver listas de trabajos

En OpenManage Enterprise, haga clic en **Monitorear** > **Trabajos** para ver la lista de trabajos existentes. La información sobre los trabajos se proporciona en las siguientes columnas:

- **Estado del trabajo**: proporciona el estado de ejecución de un trabajo.

  Consulte Descripción del tipo de trabajo y del estado del trabajo en la página 129.

- **Estado**: proporciona el estado de un trabajo. Las opciones disponibles son Activado o Desactivado.
- **Nombre del trabajo**: nombre de un trabajo.
- **Tipo de trabajo**: proporciona el tipo de un trabajo.

Consulte Descripción del tipo de trabajo y del estado del trabajo en la página 129.

- **Descripción**: descripción detallada de un trabajo.
- **Última ejecución**: último período de ejecución de un trabajo.

Los trabajos también se pueden filtrar ingresando o seleccionando los valores en la sección **Filtros avanzados**. La siguiente información adicional se puede proporcionar para filtrar las alertas:

- **Fecha de inicio de la última ejecución:** fecha de inicio de la última ejecución de los trabajos.
- **Fecha de finalización de la última ejecución**: fecha de finalización de la última ejecución de los trabajos.
- **Fuente**: las opciones disponibles son Todos, Generado por el usuario (predeterminado) y Sistema.

Para ver más información sobre un trabajo, seleccione un trabajo y, a continuación, haga clic en **Ver detalles** en el panel derecho. Consulte Visualizar la información de trabajos individuales en la página 132.

OpenManage Enterprise ofrece un informe integrado para ver la lista de trabajos programados. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Informes** > **Informe de trabajos programados**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

NOTA: En las páginas **Programas de detección e inventario**, el estado de un trabajo programado se identifica como **En cola** en la columna **ESTADO**. Sin embargo, el mismo estado se indica como **Programado** en la página **Trabajos**.

Descripción del tipo de trabajo y del estado del trabajo

Tabla 21. Estado y descripción del trabajo

Estado del trabajo	Descripción
Programado	El trabajo está programado para ejecutarse en una fecha u hora posterior.
En cola	Trabajos en espera de ejecución.
Starting (Iniciando)	
En ejecución	El trabajo se activa mediante **Ejecutar ahora**
Completo	El trabajo se ejecutó.
Error	La ejecución del trabajo no se realizó correctamente.
Nuevo	El trabajo se creó, pero no se ejecutado.
Finalizado con errores	La ejecución del trabajo fue parcialmente correcta y se completó con errores.
Anulado	El usuario pausó la ejecución del trabajo.
Paused (En pausa)	El usuario detuvo la ejecución del trabajo.
Detenido	El usuario interrumpió la ejecución del trabajo.
Cancelado	
No ejecutado	El trabajo está en cola o programado, y todavía no se ha ejecutado.

Un trabajo puede pertenecer a cualquiera de los siguientes tipos:

Tabla 22. Tipos y descripción del trabajo

Tipo de trabajo	Descripción
Estado	Revisa el estado de los dispositivos. Consulte Estados de los dispositivos en la página 39.
Inventario	Crea el informe de inventario de los dispositivos. Consulte Administración del inventario del dispositivo en la página 72.
Configuración de dispositivo	Crea la línea base de cumplimiento de una configuración de dispositivo. Consulte Administración del cumplimiento de la configuración del dispositivo en la página 109.
Report_Task	Crea informes acerca de los dispositivos mediante el uso de campos de datos integrados o personalizados. Consulte Informes en la página 138.
Garantía	Genera datos acerca del estado de garantía de los dispositivos. Consulte Administración de la garantía del dispositivo en la página 136.

Tabla 22. Tipos y descripción del trabajo (continuación)

Tipo de trabajo	Descripción
Onboarding_Task	Integra los dispositivos detectados. Consulte Incorporación de dispositivos en la página 44.
Detección	Detecta dispositivos. Consulte Detección de dispositivos para la supervisión o administración en la página 40.
Tarea de ejecución de actualización de la consola	El trabajo de actualización de la consola se rastrea mediante esta tarea. Esta tarea ayuda a identificar si la actualización se completó o presentó un error.
Copias de seguridad	
Perfiles de chasis	
Registros de depuración	Recopila los registros de depuración de las tareas de monitoreo de la aplicación, los eventos y el historial de ejecución de tareas.
Acción del dispositivo	Crea acciones en los dispositivos, como Encender LED, Apagar LED, CLI de IPMI, CLI de RACADM, etc.
Diagnostic_Task	La descarga o ejecución de tareas de diagnóstico/TSR o SupportAssist están relacionadas con la tarea de diagnóstico. Consulte Ejecución y descarga de informes de diagnóstico.
Importar definición de VLAN	Importación de definiciones de VLAN desde Excel o MSM.
Proveedor de OpenID Connect	Configuración de la conexión de OpenID. Consulte Inicio de sesión en OpenManage Enterprise mediante proveedores de OpenID Connect.Inicio de sesión en OpenManage Enterprise mediante proveedores de OpenID Connect en la página 158
PluginDownload_Task	Se realiza un seguimiento de la tarea de descarga de plug-ins y esta tarea ayuda a identificar si la descarga de plug-ins de RPM se ha completado y está lista para su instalación. Consulte Comprobación y actualización de la versión de OpenManage Enterprise y las extensiones disponibles.
Post_Upgrade_Task	Se realiza un seguimiento de la tarea PostUpgrade para establecer los ajustes de los dispositivos realizados en la versión N-1 o N-2 y también se ejecuta la tarea de detección que se creó en la versión anterior para asegurarse de que todos los dispositivos aparezcan en la lista.
Report_Task	Se realiza un seguimiento de la tarea de informe cuando el usuario ejecuta el informe (tanto para los predefinidos como para los personalizados).
Restaurar	
Actualización de la configuración	Se realiza un seguimiento de la tarea de actualización de la configuración cuando el usuario aplica una nueva configuración en la pestaña Ajustes de la aplicación.
Reversión de software	Se realiza un seguimiento de la tarea de reversión cuando el usuario realiza una operación de reversión en un dispositivo objetivo.
Actualizar	Se realiza un seguimiento de la tarea de actualización cuando el usuario realiza la actualización del firmware o del controlador en los dispositivos objetivo.
Upgrade_Bundle_Download_Task	Se realiza un seguimiento de la tarea de descarga del paquete de actualización y esta tarea ayuda a identificar si la descarga de OMEnterprise RPM se ha completado y está lista para su instalación.

Programa y trabajos predeterminados de OpenManage Enterprise

OpenManage Enterprise tiene muchos trabajos de mantenimiento internos que el dispositivo activa automáticamente en un programa establecido.

Tabla 23. En la siguiente tabla, se enumeran los nombres predeterminados de los trabajos de OpenManage Enterprise junto con su programa.

Nombre del trabajo	Expresión Cron	Descripción de la expresión Cron	Ejemplo
Inventario de configuración	0 0 0 1/1 * ? *	A las 00:00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mié May 19 00:00:00 UTC 2021
Tarea de actualización de la consola predeterminada	0 0 12 ? * LUN *	A las 12:00:00 p. m., todos los lunes, todos los meses	• Lun May 24 12:00:00 UTC 2021 • Lun May 31 12:00:00 UTC 2021
Tarea de inventario predeterminada	0 0 5 * * ? *	A las 05:00:00 a. m. todos los días	• Mar May 18 05:00:00 UTC 2021 • Mié May 19 05:00:00 UTC 2021
Tarea de depuración de configuración de dispositivos para la limpieza	0 0/1 * * * ? *	En el segundo :00, cada minuto a partir del minuto :00 de cada hora	• Lun May 17 18:39:00 UTC 2021 • Lun May 17 18:40:00 UTC 2021
Tarea de depuración de archivos para uso compartido	0 0 0 1/1 * ? *	A las 00:00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mié May 19 00:00:00 UTC 2021
Tarea de depuración de archivos para archivos de DUP únicos	0 0 0/4 1/1 * ? *	En el segundo :00, en el minuto :00, cada cuatro horas a partir de las 00:00 a. m., todos los días a partir del 1, cada mes	• Lun May 17 20:00:00 UTC 2021 • Mar May 18 00:00:00 UTC 2021 • Mar May 18 04:00:00 UTC 2021 • Mar May 18 04:00:00 UTC 2021
Tarea de estado global	0 0 0/1 1/1 * ? *	En el segundo :00, en el minuto :00, cada hora a partir de las 00:00 a. m., todos los días a partir del 1, cada mes	• Lun May 17 19:00:00 UTC 2021 • Lun May 17 20:00:00 UTC 2021
Tarea de sincronización interna	0 0/5 * 1/1 * ? *	En el segundo :00, cada cinco minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 18:45:00 UTC 2021 • Lun May 17 18:50:00 UTC 2021
Tarea de depuración de métricas	0 0 * ? * *	En el segundo :00 del minuto :00 de cada hora	• Lun May 17 19:00:00 UTC 2021 • Lun May 17 20:00:00 UTC 2021 • Lun May 17 21:00:00 UTC 2021
Tarea de métricas	0 0/15 * 1/1 * ? *	En el segundo :00, cada 15 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 18:45:00 UTC 2021 • Lun May 17 19:00:00 UTC 2021
Tarea de suscripción móvil	0 0/2 * 1/1 * ? *	En el segundo :00, cada 2 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 18:54:00 UTC 2021 • Lun May 17 18:56:00 UTC 2021
Tarea de detección iniciada por el nodo	0 0/10 * 1/1 * ? *	En el segundo :00, cada 10 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 19:00:00 UTC 2021 • Lun May 17 19:10:00 UTC 2021
Tarea de rotación de contraseña	0 0 0/6 1/1 * ? *	En el segundo :00, en el minuto :00, cada 6 horas a partir de las 00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mar May 18 06:00:00 UTC 2021 • Mar May 18 12:00:00 UTC 2021
Registro de métricas periódicas	0 0 3 * * ?	A las 03:00:00 a. m. todos los días	• Mar May 18 03:00:00 UTC 2021 • Mié May 19 03:00:00 UTC 2021
Tarea de análisis de mantenimiento a petición de depuración para la tabla: tarea	0 0 0/5 1/1 * ? *	En el segundo :00, en el minuto :00, cada 5 horas a partir de las 00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mar May 18 05:00:00 UTC 2021 • Mar May 18 10:00:00 UTC 2021

Tabla 23. En la siguiente tabla, se enumeran los nombres predeterminados de los trabajos de OpenManage Enterprise junto con su programa. (continuación)

Nombre del trabajo	Expresión Cron	Descripción de la expresión Cron	Ejemplo
Tabla de tareas de depuración: Event_Archive	0 0 18/12 ? * * *	En el segundo :00, en el minuto :00, cada 12 horas a partir de las 18 p. m., de cada día	• Mar May 18 18:00:00 UTC 2021 • Mié May 19 18:00:00 UTC 2021 • Jue May 20 18:00:00 UTC 2021
Tabla de tareas de depuración: Group_Audit	0 0 0 1/1 * ? *	A las 00:00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mié May 19 00:00:00 UTC 2021 • Jue May 20 00:00:00 UTC 2021
Tabla de tareas de depuración: tarea	0 0 0 1/1 * ? *	A las 00:00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mié May 19 00:00:00 UTC 2021 • Jue May 20 00:00:00 UTC 2021
Tabla de tareas de depuración: announced_target	0 0 0 1/1 * ? *	A las 00:00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mié May 19 00:00:00 UTC 2021 • Jue May 20 00:00:00 UTC 2021
Tarea de depuración para la tabla: registro de aplicación principal	0 0 0/5 1/1 * ? *	En el segundo :00, en el minuto :00, cada 5 horas a partir de las 00:00 a. m., todos los días a partir del 1, cada mes	• Mar May 18 00:00:00 UTC 2021 • Mar May 18 05:00:00 UTC 2021
Tarea de depuración para la tabla: evento	0 0/30 * 1/1 * ? *	En el segundo :00, cada 30 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 19:30:00 UTC 2021 • Lun May 17 20:00:00 UTC 2021 • Lun May 17 20:30:00 UTC 2021
Tarea de depuración para la tabla: dispositivo de infraestructura	0 0/30 * 1/1 * ? *	En el segundo :00, cada 30 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 19:30:00 UTC 2021 • Lun May 17 20:00:00 UTC 2021 • Lun May 17 20:30:00 UTC 2021
Tarea de sondeo de suscripción	0 0/30 * 1/1 * ? *	En el segundo :00, cada 30 minutos a partir del minuto :00, cada hora, cada día a partir del 1, cada mes	• Lun May 17 19:30:00 UTC 2021 • Lun May 17 20:00:00 UTC 2021 • Lun May 17 20:30:00 UTC 2021

Visualizar la información de trabajos individuales

1. En la página **Trabajos**, seleccione la casilla de verificación correspondiente al trabajo.
2. En el panel derecho, haga clic en **Ver detalles**.
   En la página **Detalles del trabajo**, se muestra la información del trabajo.
3. Haga clic en **Reiniciar trabajo** si el estado de un trabajo cualquiera se encuentra dentro de las siguientes opciones: Detenido, En error o Nuevo.
   Aparecerá un mensaje que indica que se ha iniciado la ejecución del trabajo.

   En la sección **Historial de ejecución** se indica la información sobre de la fecha en que el trabajo se ejecutó correctamente. En la sección **Detalles de ejecución** se indican los dispositivos en que se ejecutó el trabajo y cuánto tiempo tardó.

   NOTA: Si se detiene una tarea de corrección de configuración, el estado general de la tarea se indica como "Detenido", pero la tarea continúa ejecutándose. Sin embargo, en la sección **Historial de ejecución**, el estado se indica como en ejecución.
4. Para exportar datos a un archivo de Excel, seleccione todas las casillas de verificación o solo las correspondientes y, a continuación, haga clic en **Exportar**. Consulte Exportar todos los datos o aquellos seleccionados en la página 66.

Crear un trabajo para encender los LED del dispositivo

En los siguientes pasos, se describe cómo hacer parpadear los LED de los dispositivos especificados con el asistente para Hacer parpadear los dispositivos.

Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16

1. El asistente para Hacer parpadear los dispositivos se puede activar de las siguientes maneras:
   a. Desde la página Trabajos (**OpenManage Enterprise** > **Monitorear** > **Trabajos**), haga clic en **Crear** y, luego, seleccione **Hacer parpadear los dispositivos**.
   b. Desde la página Todos los dispositivos (**OpenManage Enterprise** > **Dispositivos**), seleccione los dispositivos y haga clic en el menú desplegable **Más acciones** y, luego, en **Encender LED** o **Apagar LED**.
2. En el cuadro de diálogo **Asistente para hacer parpadear los dispositivos**:
   a. En la sección **Opciones**:
      i. En la casilla **Nombre del trabajo**, ingrese el nombre del trabajo.
      ii. En el menú desplegable **Duración de parpadeo del LED**, seleccione las opciones para hacer parpadear el LED durante un intervalo establecido, para encenderlo o para apagarlo.
      iii. Haga clic en **Siguiente**.
   b. En la sección **Destino**, seleccione los dispositivos o grupos de destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.
   c. En el menú desplegable **Programa**, seleccione **Ejecutar ahora**, **Ejecutar más tarde** o **Ejecutar según el programa**. Consulte Definiciones de los campos Programar trabajos en la página 179.
3. Haga clic en **Finish** (Finalizar).
   Se crea un trabajo de parpadeo de LED que aparece en la página Trabajos (**OpenManage Enterprise** > **Monitorear** > **Trabajos**) y la columna **ESTADO DE TRABAJO**.

Crear un trabajo para administrar dispositivos de alimentación

NOTA: Las acciones de control de la alimentación solo se pueden realizar en dispositivos descubiertos y administrados mediante iDRAC (fuera de banda).

1. Haga clic en **Crear** y, a continuación, seleccione **Dispositivos de control de alimentación**.
2. En el cuadro de diálogo **Asistente para dispositivos de control de alimentación**:
   a. En la sección **Opciones**:
      i. Ingrese el nombre del trabajo en **Nombre del trabajo**.
      ii. En el menú desplegable **Opciones de alimentación**, seleccione cualquiera de las tareas: **Encender**, **Apagar** o **Realizar el ciclo de apagado y encendido**.
      iii. Haga clic en **Siguiente**.
   b. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.
   c. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos en la página 179.
3. Haga clic en **Finalizar**.
   El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
4. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
   - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
   - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.
   - Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Visualizar la información de trabajos individuales en la página 132.

Crear un trabajo de comando remoto para la administración de dispositivos

Mediante el asistente de trabajos de la línea de comandos, puede crear trabajos de comandos remotos a fin de administrar los dispositivos objetivo de manera remota.

1. Haga clic en **Crear** y, a continuación, seleccione **Comando remoto en dispositivos**.
2. En el cuadro de diálogo **Asistente para trabajos de línea de comandos** en la sección **Opciones**:
   a. Ingrese el nombre del trabajo en **Nombre del trabajo**.
   b. En el menú desplegable Interfaz, seleccione una de las interfaces según los dispositivos objetivo que desea administrar:
      - **CLI de IPMI**: para los servidores que no son de Dell y los iDRAC.
      - **CLI de RACADM**: para los iDRAC detectados mediante el protocolo WSMAN.
      - **CLI de SSH**: para servidores Linux detectados mediante el protocolo SSH.
   c. En el cuadro **Argumentos**, ingrese el comando. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.

      NOTA: Los comandos del cuadro Argumentos se ejecutan uno a la vez.

   d. Haga clic en **Siguiente**.
      Una marca visto verde junto a **Opciones** indica que se han proporcionado los datos necesarios.
3. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte Definiciones de los campos Programar trabajos en la página 179.
5. Haga clic en **Finalizar**.
   El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
6. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
   - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
   - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.
   - Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Visualizar la información de trabajos individuales en la página 132.

Crear un trabajo para cambiar el tipo de complemento de la consola virtual

Puede cambiar el tipo de complemento de consola virtual a HTML5 en varios dispositivos. La actualización a HTML5 puede dar como resultado una mejor experiencia de navegador. Para actualizar, haga lo siguiente:

1. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Trabajos**
2. Haga clic en **Crear** y, a continuación, seleccione **Cambiar complemento de la consola virtual en los dispositivos**.
3. En el cuadro de diálogo **Asistente para cambiar el complemento de la consola virtual**, en la sección **Opciones**:
   a. Ingrese el nombre del trabajo en **Nombre del trabajo**. De manera predeterminada, el tipo de complemento se muestra como HTML5.
   b. Haga clic en **Siguiente**.
4. En la sección **Destino del trabajo**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino en la página 135.
   a. Haga clic en **Siguiente**.
5. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos en la página 179.
6. Haga clic en **Finalizar**.
   El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
7. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
   - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
   - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.
   - Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Visualizar la información de trabajos individuales en la página 132.

Seleccionar dispositivos y grupos de dispositivos de destino

De manera predeterminada, se selecciona la opción **Seleccionar dispositivos** para indicar que el trabajo se puede ejecutar en los dispositivos. También puede ejecutar un trabajo en los grupos de dispositivos mediante la selección de **Seleccionar grupos**.

NOTA: Los grupos de dispositivos y los dispositivos que se muestran se rigen por el acceso operativo basado en el alcance que tiene el usuario para los dispositivos. Para obtener más información, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Haga clic en **Seleccionar dispositivos**.

   En el cuadro de diálogo **Destino del trabajo**, el panel izquierdo muestra una lista de los dispositivos supervisados por OpenManage Enterprise. En el panel de trabajo, se muestran una lista de dispositivos relacionados con cada grupo y los detalles del dispositivo. Para obtener descripciones sobre campos, consulte Página Todos los dispositivos: lista de dispositivos en la página 61. Para obtener información acerca de los grupos de dispositivos, consulte Organizar los dispositivos en grupos en la página 54.
2. Seleccione la casilla de verificación correspondiente al dispositivo y haga clic en **Aceptar**.
   Los dispositivos seleccionados se muestran en la sección **Todos los dispositivos seleccionados** del grupo seleccionado.

Administrar los trabajos

Una vez que se hayan creado los trabajos y se muestren en la página **Trabajos**, podrá administrarlos de la siguiente manera.

- **Ejecutar trabajos**: seleccione la casilla de verificación correspondiente a un trabajo y, luego, haga clic en **Ejecutar ahora** para ejecutar la tarea en los dispositivos objetivo. Puede ejecutar un trabajo cuando se encuentra en estado activado.
- **Activar trabajos**: seleccione la casilla de verificación correspondiente a un trabajo y, luego, haga clic en **Activar**.
- **Desactivar trabajos**: seleccione la casilla de verificación correspondiente a un trabajo y, luego, haga clic en **Desactivar**.
  NOTA: Solo se puede deshabilitar la ejecución de los trabajos “programados”. Los trabajos que están activos y en el estado “en ejecución” no se pueden desactivar en la mitad del proceso.
- **Detener trabajos**: seleccione la casilla de verificación correspondiente a un trabajo y, luego, haga clic en **Detener**. Puede detener un trabajo cuando se encuentra en ejecución.
- **Eliminar**: seleccione la casilla de verificación correspondiente a un trabajo y, luego, haga clic en **Eliminar**.

17

Administración de la garantía del dispositivo

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Haga clic en **OpenManage Enterprise** > **Monitoreo** > **Garantía** para ver los estados de garantía de todos los dispositivos que se monitorean con OpenManage Enterprise dentro de su alcance. Por ejemplo, un administrador con acceso a todos los grupos de dispositivos verá los detalles de la garantía de todos los dispositivos, mientras que los administradores de dispositivos solo verán los detalles de la garantía de los dispositivos que se encuentran dentro de su alcance correspondiente.

También puede exportar datos seleccionados o todos los datos a una hoja de Excel para fines estadísticos y de análisis. En la página Garantía se muestran los siguientes detalles:

- **ESTADO** de la garantía
  NOTA: El estado de la garantía está determinado por la configuración que seleccione el administrador. Consulte Administración de la configuración de garantía en la página 167
  -  significa **crítico**, que indica que la garantía ha caducado.
  -  significa **advertencia**, lo que indica que la garantía se acerca al vencimiento.
  -  significa **normal**, lo que indica que la garantía está activa.
- **ETIQUETA DE SERVICIO**
- **MODELO DEL DISPOSITIVO**
- **TIPO DE DISPOSITIVO**
- **TIPO DE GARANTÍA**:
  - Inicial: la garantía entregada con la compra de OpenManage Enterprise.
  - Extendida: la garantía se extiende, ya que la duración de la garantía inicial expiró.
- **DESCRIPCIÓN DEL NIVEL DE SERVICIO**: indica el Acuerdo de nivel de servicio (SLA) asociado con la garantía del dispositivo.
- **DÍAS RESTANTES**: cantidad de días que faltan para que venza la garantía. Puede establecer los días para recibir una alerta antes de que la garantía caduque. Consulte Administración de la configuración de garantía en la página 167.

OpenManage Enterprise ofrece un informe incorporado sobre las garantías que vencen en los próximos 30 días. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Informes** > **Garantías que vencen en los próximos 30 días**. Haga clic en **Ejecutar**. Consulte Ejecutar informes en la página 139.

Para filtrar los datos que se muestran en la tabla, haga clic en **Filtros avanzados**. Consulte acerca de la sección de filtros avanzados Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise en la página 35.

El estado de garantía de todos los dispositivos descubiertos se recopila automáticamente una vez por semana mediante un trabajo de garantía incorporado. También puede iniciar manualmente el trabajo de garantía haciendo clic en **Actualizar garantía** en la esquina superior derecha.

Para exportar todo o los datos de la garantía seleccionados, haga clic en **Exportar**. Consulte Exportar todos los datos o aquellos seleccionados en la página 66.

Tareas relacionadas

Ver y renovar la garantía del dispositivo en la página 137

Temas:

Ver y renovar la garantía del dispositivo

Haga clic en **OpenManage Enterprise** > **Supervisión** > **Garantía** para obtener una lista de los estados de la garantía de todos los dispositivos supervisados por OpenManage Enterprise, junto con la etiqueta de servicio, el nombre del modelo, el tipo de dispositivo, la garantía asociada y la información del nivel de servicio. Para obtener descripciones sobre campos, consulte Administración de la garantía del dispositivo en la página 136.

Para ver la información sobre la garantía y para renovar la garantía de un dispositivo:

- Seleccione la casilla de verificación correspondiente al dispositivo. En el panel derecho, se muestra el estado de la garantía y otros detalles importantes del dispositivo, como el código del nivel de servicio, el proveedor de servicios, la fecha de inicio de la garantía, la fecha de término de la garantía, etc.
- Las garantías caducadas se pueden renovar haciendo clic en **Renovación de la garantía de Dell para el dispositivo**. Esta acción lo llevará al sitio de soporte de Dell EMC, en el que podrá administrar la garantía del dispositivo.
- Haga clic en **Actualizar garantía** en la esquina superior derecha para actualizar la tabla Garantía. Los estados de la garantía cambian automáticamente de crítico  a normal  para todos los dispositivos cuyas garantías se renuevan. Cada vez que se hace clic en **Actualizar garantía**, se genera un nuevo registro de alertas de la Garantía del dispositivo con el número total de garantías vencidas en la consola. Para obtener información sobre los registros de alertas, consulte Ver los registros de alertas
- Para ordenar los datos de la tabla en función de una columna, haga clic en el título de la columna.
- Haga clic en el botón **Filtros avanzados** para personalizar.

Información relacionada

Administración de la garantía del dispositivo en la página 136

18

Informes

Si hace clic en **OpenManage Enterprise** > **Supervisión** > **Informes**, puede generar informes personalizados para ver los detalles del dispositivo en profundidad. Los informes permiten ver datos acerca de los dispositivos, trabajos, alertas y otros elementos del centro de datos. El usuario puede incorporar y definir los informes. Puede editar o eliminar solo los informes definidos por el usuario. Las definiciones y criterios utilizados para un informe incorporado no se pueden editar ni eliminar. En el panel derecho se muestra una vista previa del informe que selecciona en la lista de informes.

Los informes y los datos que se muestran en la página Informes dependen de los privilegios de usuario basados en el alcance que tenga en OpenManage Enterprise. Por ejemplo, los administradores de dispositivos solo tienen acceso a los informes que crearon, además de los informes incorporados. Además, el informe que genera el usuario incluirá datos solo de los dispositivos que están dentro del alcance de ese usuario. Por ejemplo, los informes que genera el administrador y los administradores de dispositivos "sin restricciones" incluirán datos sobre todos los grupos de dispositivos. Sin embargo, los informes que generan los administradores de dispositivos que tienen un alcance restringido incluirán datos relacionados únicamente con los dispositivos o grupos de dispositivos que se encuentran dentro de su alcance.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Tabla 24. Privilegios de acceso basado en roles para administrar informes en OpenManage Enterprise

Rol de usuario:	Tareas permitidas en los informes:
Administradores y administradores de dispositivos	Ejecutar, crear, editar, copiar, enviar por correo electrónico, descargar, y exportar
Lectores	Ejecutar, enviar por correo electrónico, exportar, ver y descargar

Ventajas de la característica de informes:

- Generar un criterio de informe mediante la utilización de hasta 20 filtros
- Puede filtrar los datos y organizarlos por nombres de columnas de su preferencia
- Los informes se pueden ver, descargar y enviar por mensaje de correo electrónico
- Enviar informes para un máximo de 20 a 30 destinatarios a la vez
- Si considera que la creación del informe está tardando demasiado, puede detener el proceso
- Los informes generados se traducen automáticamente al idioma seleccionado durante la instalación de OpenManage Enterprise
- Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe

Actualmente, se pueden generar los siguientes informes incorporados para extraer información sobre lo siguiente:

- Categoría de dispositivo: activo, FRU, firmware, cumplimiento del firmware/controlador, trabajos programados, resumen de alertas, unidad de disco duro, gabinete modular, NIC, unidad virtual, garantía y licencia.
- Categoría de alertas: alertas semanales

Tareas relacionadas

Ejecutar informes en la página 139
Generación de informes y su envío a través de correo electrónico en la página 139
Editar informes en la página 140
Eliminar informes en la página 140

Temas:

- Creación de informes
- Exportación de informes seleccionados

Ejecutar informes

En la página Informes (**OpenManage Enterprise** > **Monitorear** > **Informes**), puede ejecutar, ver y descargar los informes incorporados o los informes que haya creado.

Cuando se ejecuta un informe, se muestran las primeras 20 filas y se pueden paginar los resultados paginados. Para ver todas las filas a la vez, descargue el informe. Para editar este valor, consulte Exportar todos los datos o aquellos seleccionados en la página 66. Los datos que se muestran en la salida no se pueden ordenar, ya que así está definido en la consulta que se utiliza para crear un informe. Para ordenar los datos, edite la consulta de informe o expórtelos a una hoja de Excel. Nota: Se recomienda no ejecutar más de cinco (5) informes a la vez, ya que la generación de informes consume recursos del sistema. Sin embargo, este valor de cinco informes depende de los dispositivos descubiertos, los campos utilizados y la cantidad de tablas que se han unido para generar el informe. Se crea una tarea y se ejecuta cuando se solicita la generación de un informe. Para conocer los privilegios basados en roles necesarios para generar informes, consulte Creación de informes en la página 141.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Los informes que genera el administrador de dispositivos solo tendrán datos correspondientes a los dispositivos que se encuentran dentro de su alcance.
- No se recomienda ejecutar informes con frecuencia, ya que consume recursos de datos y de procesamiento.
- Para un informe cuya categoría es "Dispositivo", las primeras columnas, de forma predeterminada, son Nombre del dispositivo, Modelo del dispositivo y Etiqueta de servicio del dispositivo. Puede excluir las columnas mientras se personaliza el informe.

Para ejecutar un informe, seleccione el informe y haga clic en **Ejecutar**. En la página **Informes de <report name>**, el informe se tabula utilizando los campos que están definidos para crear el informe.

Para descargar un informe, realice lo siguiente:

1. Haga clic en **Descargar**.
2. En el cuadro de diálogo **Descargar el informe**, seleccione el tipo de archivo de salida y haga clic en **Finalizar**. Se muestra el archivo de salida seleccionado. Actualmente, puede exportar un informe a formatos de archivos CVS, XML, PDF, y Excel. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Para enviar el informe por correo electrónico, realice lo siguiente:

1. Haga clic en **Correo electrónico**.
2. En el cuadro de diálogo **Enviar informe por correo electrónico**, seleccione el formato de archivo, escriba la dirección de correo electrónico del receptor y, a continuación, haga clic en **Finalizar**. El informe se envía por correo electrónico. Puede enviar informes por correo electrónicos de 20 a 30 destinatarios a la vez.
3. Si la dirección de correo electrónico no está configurada, haga clic en **Ir a la configuración de SMTP**. Para obtener más información sobre la configuración de las propiedades de SMTP, consulte Configuración de credenciales de SNMP en la página 167.

NOTA: Si va a descargar o ejecutar un informe que ya se generó, y otro usuario intenta eliminar ese informe al mismo tiempo, ambas tareas se llevan a cabo correctamente.

Información relacionada

Informes en la página 138

Generación de informes y su envío a través de correo electrónico

Puede ejecutar el informe y enviarlo por correo electrónico a una cantidad de 20 a 30 destinatarios a la vez.

NOTA: La operación de correo electrónico puede fallar con informes grandes si el tamaño del mensaje excede el tamaño de mensaje fijo establecido en el servidor SMTP. En esos casos, considere restablecer el límite de tamaño de mensaje del servidor SMTP y vuelva a intentarlo.

1. Seleccione el informe y haga clic en **Ejecutar y enviar por correo electrónico**.
2. En el cuadro de diálogo **Enviar informe por correo electrónico**:
   a. En el menú desplegable **Formato**, seleccione uno de los formatos de archivo en que se debe generar el informe: HTML, CSV, PDF o MS-Excel.
   b. En la casilla **Para**, ingrese la dirección de correo electrónico del destinatario. Si la dirección de correo electrónico no está configurada, haga clic en **Ir a la configuración de SMTP**. Para obtener más información sobre la configuración de las propiedades de SMTP, consulte Configuración de credenciales de SNMP en la página 167.
   c. Haga clic en **Finalizar**.
   El informe se envía por correo electrónico y se registra en los registros de auditoría.

Información relacionada

Informes en la página 138

Editar informes

Solo se pueden editar los informes creados por el usuario.

1. Seleccione el informe y haga clic en **Editar**.
2. En el cuadro de diálogo **Definición de informe**, edite la configuración. Consulte Creación de informes.
3. Haga clic en **Guardar**.
   Se guarda la información actualizada. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.
   NOTA: Cuando edita un informe personalizado, si la categoría se cambia, los campos asociados también se eliminan.

Información relacionada

Informes en la página 138

Copia de informes

Solo se pueden copiar los informes creados por el usuario.

1. Seleccione el informe, haga clic en **Más acciones** y, a continuación, haga clic en **Copiar**.
2. En el cuadro de diálogo **Copiar definición de informe**, ingrese un nuevo nombre para el informe copiado.
3. Haga clic en **Guardar**.
   Se guarda la información actualizada. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Eliminar informes

Solo se pueden eliminar los informes creados por el usuario. Si se elimina una definición de informe, se elimina también el historial de informes asociados y se detiene cualquier ejecución de un informe que esté utilizando esa definición de informe.

1. En el menú **OpenManage Enterprise**, en **Supervisión**, seleccione **Informes**.
   Se muestra una lista de informes disponibles de dispositivos.
2. Seleccione el informe, haga clic en **Más acciones** y, a continuación, haga clic en **Eliminar**.
   NOTA: Si va a descargar o ejecutar un informe que ya se generó, y otro usuario intenta eliminar ese informe al mismo tiempo, ambas tareas se llevan a cabo correctamente.
3. En el cuadro de diálogo **Eliminar definición de informe**, cuando se le pregunte si desea eliminar o no el informe, haga clic en **Sí**.
   El informe se elimina de la lista de informes y la tabla se actualiza. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Información relacionada

Informes en la página 138

Creación de informes

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Los informes que genera el administrador de dispositivos solo tendrán datos correspondientes a los grupos de dispositivos que se encuentran dentro de su alcance.
- Algunas tablas contienen datos específicos del tipo de dispositivo que bloquearán de manera efectiva el informe para ese tipo de dispositivo. La combinación de columnas de tablas específicas de múltiples dispositivos de diferentes tipos (por ejemplo, servidores y chasis) dará como resultado un informe no válido sin resultados.

Si bien los informes integrados tienen definiciones predeterminadas (criterios de filtro) para generar informes, puede personalizar los criterios para crear sus propias definiciones y generar informes personalizados. Los campos o columnas que desee incluir en el informe dependen de la categoría que seleccione. Puede seleccionar solo una categoría a la vez. La disposición de las columnas de un informe se puede modificar mediante la acción de arrastrar y colocar. También:

- Los nombres de los informes deben ser únicos
- La definición del informe debe tener al menos un campo y una categoría
- Para los informes que tienen Dispositivo y Alerta como categorías, el nombre del dispositivo o el grupo de dispositivos debe ser uno de los campos obligatorios

De manera predeterminada, **Dispositivos** se selecciona como categoría, y las columnas de nombre de dispositivo, etiqueta de servicio del dispositivo y modelo del dispositivo se muestran en el panel de trabajo. Si selecciona cualquier otra categoría mientras edita los criterios de un informe, se muestra un mensaje que indica que los campos predeterminados se eliminarán. Cada categoría tiene propiedades predefinidas que se pueden usar como títulos de columnas en las que los datos se filtran según los criterios que usted defina. Ejemplo de tipos de categorías:

- Trabajos: nombre de la tarea, tipo de tarea, estado de la tarea y tarea interna.
- Grupos: estado del grupo, descripción del grupo, tipo de membresía del grupo, nombre del grupo y tipo de grupo.
- Alertas: estado de la alerta, gravedad de la alerta, nombre del catálogo, tipo de alerta, subcategoría de la alerta e información del dispositivo.
- Dispositivos: alerta, catálogo de alerta, ventilador del chasis, software del dispositivo, etc. Estos criterios tienen clasificaciones adicionales según los datos que se pueden filtrar y los informes que se pueden generar.

Tabla 25. Privilegios de acceso basado en roles para generar informes en OpenManage Enterprise

Rol de usuario:	Tareas permitidas en los informes:
Administradores y administradores de dispositivos	Ejecutar, crear, editar, copiar, enviar por correo electrónico, descargar, y exportar
Lectores	Ejecutar, enviar por correo electrónico, exportar, ver y descargar

1. Haga clic en **Informes** > **Crear**.
2. En el cuadro de diálogo **Definición de informe**:
   a. Escriba el nombre y la descripción del nuevo informe que desea definir.
   b. Haga clic en **Siguiente**.
3. En la sección **Generador de informes**:
   a. En el menú desplegable **Categoría**, seleccione la categoría del informe.
      - Si selecciona Dispositivo como categoría, seleccione el grupo de dispositivos también.
      - Si es necesario, modifique los criterios de filtro. Consulte Seleccionar los criterios de una consulta en la página 57.
   b. En la sección **Columnas**, seleccione las casillas de verificación de los campos que deben aparecer como columnas en el informe. Los nombres de los campos seleccionados se muestran en la sección **Orden de columnas**.
   c. Puede personalizar el informe de las siguientes formas
      - Usando los cuadros **Ordenar por** y **Dirección**.

- Arrastrando los campos hacia arriba o hacia abajo en la sección **Orden de columnas**.

4. Haga clic en **Finish** (Finalizar).
   El informe se genera y aparece en la lista de informes. Puede exportar el informe para fines de análisis. Consulte Exportar todos los datos o aquellos seleccionados en la página 66. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Seleccionar criterios de consulta durante la creación de informes

Defina filtros cuando cree criterios de consulta para:

- Generación de informes personalizados. Consulte Creación de informes en la página 141.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte Crear un grupo de dispositivos de consulta en la página 57.

Defina los criterios de consulta mediante dos opciones:

- **Seleccionar consulta existente para copiar**: de manera predeterminada, OpenManage Enterprise proporciona una lista de plantillas de consulta incorporada que puede copiar y crear sus propios criterios de consulta. Cuando se define una consulta, se puede utilizar un máximo de 20 criterios (filtros). Para agregar filtros, debe seleccionar desde el menú desplegable **Seleccionar tipo**.
- **Seleccionar tipo**: cree criterios de consulta desde cero mediante los atributos que se muestran en este menú desplegable. Los elementos en el menú dependen de los dispositivos que supervisa OpenManage Enterprise. Cuando se selecciona un tipo de consulta, se muestran solo operadores adecuados como =, >, < y null según el tipo de consulta. Se recomienda este método para definir criterios de consulta durante la elaboración de informes personalizados.

  NOTA: Si se evalúa una consulta con varias condiciones, el orden de evaluación es el mismo que en SQL. Para especificar un orden en particular para la evaluación de las condiciones, agregue o quite entre paréntesis cuando defina la consulta.

NOTA: Cuando se selecciona esta opción, los filtros de los criterios de una consulta existente solo se copian virtualmente para crear un nuevo criterio de consulta. Los filtros predeterminados asociados con los criterios de una consulta existente no cambian. La definición (filtros) de criterios de consulta incorporados se utiliza como punto de partida para la creación de los criterios de una consulta personalizada. Por ejemplo:

1. *Consulta1* corresponde a criterios integrados de consulta que tiene el siguiente filtro predefinido: `Task Enabled=Yes`.
2. Copie las propiedades de filtro de *consulta1*, cree *consulta2* y, a continuación, personalice los criterios de consulta agregando otro filtro: `Task Enabled=Yes` Y `(Task Type=Discovery)`.
3. Más adelante, abra *consulta1*. Sus criterios de filtro todavía permanecen como `Task Enabled=Yes`.

1. En el cuadro de diálogo **Selección de criterios de consulta**, seleccione en el menú desplegable según si desea crear criterios de consulta para grupos de consulta o para generación de informes.
2. Agregue o quite un filtro haciendo clic en el símbolo más o en el símbolo de basurero, respectivamente.
3. Haga clic en **Finalizar**.
   Se genera un criterio de consulta y se guarda en la lista de consultas existentes. Se realiza una entrada de registro de auditoría y aparece en la lista de los registros de auditoría. Consulte Monitoreo de registros de auditoría en la página 126.

Exportación de informes seleccionados

1. Seleccione las casillas de verificación correspondientes a los informes que se deben exportar, haga clic en **Más acciones** y, a continuación, haga clic en **Exportar seleccionados**.

   En este momento, no se pueden exportar todos los informes a la vez.
2. En el cuadro de diálogo **Exportar informes seleccionados**, seleccione cualquiera de los siguientes formatos de archivo para exportar el informe: HTML, CSV o PDF.
3. Haga clic en **Finalizar**.
   En el cuadro de diálogo, abra o guarde el archivo en una ubicación conocida para fines estadísticos y de análisis.

19

Administración de archivos de MIB

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Las herramientas de terceros en su centro de datos pueden generar alertas que son vitales para sus operaciones. Estas alertas se almacenan en archivos de Base de información de administración (MIB) definidos y entendidos por herramientas de los proveedores respectivos. Sin embargo, OpenManage Enterprise también le permite administrar estas MIB, de manera que las MIB que no son de Dell EMC se puedan importar, analizar y utilizar para la administración de dispositivos en OpenManage Enterprise. OpenManage Enterprise admite SMI1 y SMI2. OpenManage Enterprise ofrece archivos de MIB integrados que se pueden utilizar para dispositivos Dell EMC. Estos son MIB solo de lectura y no se pueden editar.

NOTA: OpenManage Enterprise solo administra MIB válidos con capturas.

Puede administrar las MIB de la siguiente manera:

- Importación de archivos de MIB en la página 143
- Eliminación de archivos de MIB en la página 145
- Resolución de tipos de MIB en la página 145

Si hace clic en el menú **OpenManage Enterprise** > **Supervisión** > **MIB**, puede administrar los archivos de MIB que utiliza OpenManage Enterprise y otras herramientas de administración del sistema en el centro de datos. Una tabla indica los archivos de MIB disponibles con las siguientes propiedades. Haga clic en el encabezado de la columna para ordenar los datos.

Tabla 26. Acceso basado en funciones para archivos de MIB en OpenManage Enterprise

Funciones de OpenManage Enterprise	Control de acceso basado en roles para los archivos de MIB		
	Admin (Administrador)	Administrador de dispositivos	Observador
Ver capturas o MIB	S	S	S
Importar MIB. Editar capturas.	S	N	N
Eliminar MIB	S	N	N
Editar capturas	S	N	N

Para descargar los archivos de MIB incorporados de OpenManage Enterprise, haga clic en **Descargar MIB**. Los archivos se guardan en la carpeta especificada.

Temas:

Importación de archivos de MIB

Flujo de proceso ideal de importación de archivos de MIB: **El usuario carga los archivos de MIB en OpenManage Enterprise** > **OpenManage Enterprise analiza los archivos de MIB** > **OpenManage Enterprise realiza búsquedas en la base de datos para detectar cualquier captura similar que ya esté disponible** > **OpenManage Enterprise muestra los datos de los archivos de MIB**. El tamaño máximo de archivo de MIB que se puede importar es de 3 MB. El historial del registro de auditoría de OpenManage Enterprise guarda cada importación y eliminación de los archivos de MIB.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios de usuario basados en funciones y el acceso operativo basado en el alcance necesarios para los dispositivos. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16
- Solo se puede importar un archivo de MIB a la vez.

1. Haga clic en **MIB** > **Importar MIB**.
2. En el cuadro de diálogo, **Importar MIB**, en la sección **Cargar archivos de MIB**, haga clic en **Seleccionar archivo** para seleccionar un archivo de MIB.

   Si el MIB tiene instrucciones de importación que se resuelven mediante MIB externos, se muestra un mensaje.

   a. Haga clic en **Tipos de resolución**. Resolución de tipos de MIB. Consulte Eliminación de archivos de MIB en la página 145.
   b. Haga clic en **Finish** (Finalizar). Si el archivo de MIB es de propiedad de Dell EMC, se muestra un mensaje que indica que el MIB se incluye con el producto y no se puede modificar.
3. Haga clic en **Siguiente**.
4. En la sección **Ver capturas**, se muestra una lista de archivos de MIB con la siguiente información:
   - Categoría de alerta de la captura. Puede editar la categoría para que coincida con las definiciones de categorías de OpenManage Enterprise. Consulte Edición de capturas de MIB en la página 144.
   - El nombre de la captura es de solo lectura. Definido por el dispositivo de terceros.
   - Niveles de gravedad de una alerta: Crítica, Aviso, Información y Normal.
   - Mensaje de alerta asociado con una alerta.
   - El OID de captura es de solo lectura y único.
   - "Nuevo" indica que OpenManage Enterprise importa la captura por primera vez. Las excepciones importadas ya se indicaron como "Importadas". "Sobrescribir" indica las capturas cuya definición se vuelve a escribir a causa de una operación de importación.

   Para editar los valores predeterminados de las categorías de alerta o el nivel de gravedad de un archivo de MIB, consulte Edición de capturas de MIB en la página 144. Para eliminar archivos de MIB, seleccione las casillas de verificación correspondientes y, a continuación, haga clic en **Eliminar captura**. De este modo, los archivos de MIB se eliminan y la lista de archivos de MIB se actualiza.
5. Haga clic en **Finish** (Finalizar). Los archivos de MIB se analizan, se importan a OpenManage Enterprise y, a continuación, se enumeran en la pestaña **MIN**.

NOTA: Si importa una MIB, y después la importa de nuevo, el estado de la MIB se muestra como **IMPORTADO**. Sin embargo, si vuelve a importar un archivo de MIB que se eliminó, el estado de la captura se indica como **NUEVO**.

NOTA: Las capturas que ya fueron importadas a OpenManage Enterprise no se pueden importar.

NOTA: Los archivos de MIB incluidos de manera predeterminada con OpenManage Enterprise no se pueden importar.

NOTA: Los sucesos que se generen después de la importación de la captura se formatearán y se mostrarán de acuerdo con la nueva definición.

Edición de capturas de MIB

1. Seleccione el informe y haga clic en **Editar**.
2. En el cuadro de diálogo **Editar capturas MIB**:
   a. Seleccione o escriba datos en los campos:
      - Seleccione la nueva categoría de alerta que se asignará a la alerta. De manera predeterminada, en OpenManage Enterprise se muestran algunas categorías de alertas integradas.
      - Escriba el componente de alerta.
      - El nombre de captura es de solo lectura porque se genera mediante la herramienta de otro fabricante.
      - Seleccione la gravedad que se asignará a la alerta. De manera predeterminada, en OpenManage Enterprise se muestran algunas categorías de alertas integradas.
      - Un mensaje que describe la alerta.
   b. Haga clic en **Finalizar**.
   La captura se edita y se muestra la lista de capturas actualizada.

NOTA: No es posible editar más de una alerta a la vez. Las capturas importadas a OpenManage Enterprise no se pueden editar.

3. En el cuadro de diálogo **Definición de informe**, edite la configuración. Consulte Creación de informes.
4. Haga clic en **Guardar**.
   Se guarda la información actualizada.

Eliminación de archivos de MIB

NOTA: No es posible quitar un archivo de MIB que tiene definiciones de captura utilizadas por alguna de las directivas de alertas. Consulte Directivas de alerta en la página 120.

NOTA: Los eventos que se reciben antes de quitar un MIB no se verán afectados por el retiro del MIB asociado. Sin embargo, los eventos que se generen después del retiro tendrán capturas sin formato.

1. En la columna **NOMBRE DE ARCHIVO DE MIB**, expanda, pliegue y seleccione los archivos de MIB.
2. Haga clic en **Eliminar MIB**.
3. En el cuadro de diálogo **Eliminar MIB**, seleccione las casillas de verificación de MIB que se deben eliminar.
4. Haga clic en **Quitar**.
   De este modo, se eliminan los archivos de MIB y se actualiza la tabla de MIB.

Resolución de tipos de MIB

1. Importación de archivos de MIB. Consulte Importación de archivos de MIB en la página 143.
   Si el tipo de MIB es sin resolver, en el cuadro de diálogo **Tipos sin resolución** se muestran los tipos de MIB que indican que los tipos de MIB se importarán solo si están resueltos.
2. Haga clic en **Tipos de resolución**.
3. En el cuadro de diálogo **Tipos de resolución**, haga clic en **Seleccionar archivos** y luego seleccione los archivos faltantes.
4. En el cuadro de diálogo **Importar MIB**, haga clic en **Siguiente**. Si todavía hay tipos de MIB faltantes, el cuadro de diálogo **Tipos sin resolución** nuevamente indica los tipos de MIB faltantes. Repita los pasos 1-3.
5. Después de que se resuelvan todos los tipos de MIB sin resolución, haga clic en **Finalizar**. Complete el proceso de importación. Consulte Importación de archivos de MIB en la página 143.

Descarga de un archivo de MIB de OpenManage Enterprise

1. En la página **Supervisión**, haga clic en **MIB**.
2. Expanda y seleccione un archivo de MIB de OpenManage Enterprise y, a continuación, haga clic en **Descargar MIB**.

   NOTA: Puede descargar únicamente archivos de MIB relacionados con OpenManage Enterprise.

20

Administración de los ajustes del servidor OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Para obtener más información sobre los navegadores compatibles, consulte la *Matriz de soporte de OpenManage Enterprise* disponible en el sitio de soporte técnico.

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación**, puede:

- Configurar y administrar los ajustes de red de OpenManage Enterprise, como IPv4, IPv6, tiempo y ajustes de proxy. Consulte Configuración de red.
- Agregar, habilitar, editar y eliminar usuarios. Consulte Administración de usuarios.
- Establecer las propiedades de la condición del dispositivo y de la supervisión del panel. Consulte Administración de preferencias de la consola.
- Administrar políticas de inicio de sesión y bloqueo de usuarios. Consulte Configuración de propiedades de seguridad de inicio de sesión.
- Ver el certificado SSL actual y, a continuación, generar una solicitud de CSR. Consulte Generación y descarga de la solicitud de firma de certificado en la página 162.
- Configurar correos electrónicos, SNMP y propiedades de Syslog para la administración de alertas. Consulte Configurar alertas de SMTP, SNMP y registro del sistema en la página 122.
- Establecer un agente de escucha de SNMP y la configuración de reenvío de capturas. Consulte Administración de alertas entrantes.
- Establecer las credenciales y el tiempo que debe tardar en recibir notificaciones sobre el vencimiento de la garantía. Consulte Administración de la configuración de garantía.
- Establecer las propiedades para comprobar la disponibilidad de versiones actualizadas y, a continuación, actualizar la versión de OpenManage Enterprise. Consulte Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167.
- Establecer las credenciales de usuario para ejecutar un comando remoto mediante RACADM e IPMI. Consulte Ejecución de comandos y scripts remotos.
- Definir y recibir notificaciones de alerta en el teléfono móvil. Consulte Configuración de OpenManage Mobile en la página 174.

Tareas relacionadas

Eliminación de servicios de directorio en la página 158

Temas:

Configurar los ajustes de la red de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

1. Para ver solo la configuración actual de red de todas las conexiones de red activas de OpenManage Enterprise, como el nombre de dominio DNS, la FQDN y las configuraciones de IPv4 e IPv6, expanda **Configuración actual**.
2. Para configurar los tiempos de espera de la sesión y el número máximo de sesiones para los usuarios de la interfaz web y la API de OpenManage Enterprise, expanda **Configuración del tiempo de espera de inactividad de la sesión** y haga lo siguiente:
   a. Seleccione la casilla de verificación **Habilitar** para activar el tiempo de espera universal e ingrese el valor del **Tiempo de espera de inactividad (1-1440)**. El valor del tiempo de espera de inactividad se puede establecer entre 1 minuto y 1440 minutos (24 horas). De manera predeterminada, la espera universal aparece atenuada. Cuando se habilita el tiempo de espera universal, se deshabilitan los campos API e Interfaz web.
   b. Cambie el **Tiempo de espera de inactividad (1-1440)** de la API y los valores de **Número máximo de sesiones (1-100)**. Estos atributos se establecen de forma predeterminada en 30 minutos y 100 minutos respectivamente.
   c. Cambie el **Tiempo de espera de inactividad (1-1440)** de la interfaz web y los valores de **Número máximo de sesiones (1-100)**. Estos atributos se establecen de forma predeterminada en 30 minutos y 100 minutos respectivamente.
   d. Haga clic en **Aplicar** para guardar los ajustes o haga clic en **Descartar** para conservar los valores predeterminados.
3. Aparece la hora actual del sistema y el origen, es decir, la zona horaria local o la IP del servidor NTP. Para configurar la zona horaria del sistema, la fecha, la hora y la sincronización del servidor NTP, expanda **Configuración de hora**.
   a. Seleccione la zona horaria en la lista desplegable.
   b. Ingrese la fecha o haga clic en el icono de **calendario** para seleccionar la fecha.
   c. Ingrese la hora con el formato hh:mm:ss.
   d. Para que se sincronice con un servidor NTP, seleccione la casilla de verificación **Usar NTP** e ingrese la dirección del servidor NTP principal.

      Puede configurar hasta tres servidores NTP en OpenManage Enterprise.

      NOTA: Las opciones **Fecha** y **Hora** no están disponibles cuando la opción **Usar NTP** está seleccionada.
   e. Haga clic en **Aplicar**.
   f. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.
4. Para configurar los ajustes de proxy de OpenManage Enterprise, expanda **Configuración de proxy**.
   a. Seleccione la casilla de verificación **Activar configuración de proxy HTTP** para configurar el proxy HTTP y luego ingrese la dirección del proxy HTTP y el número de puerto HTTP.
   b. Seleccione la casilla de verificación **Habilitar autenticación de proxy** para habilitar las credenciales de proxy y, a continuación, ingrese el nombre de usuario y la contraseña.
   c. Seleccione la casilla de verificación **Ignorar validación del certificado** si el proxy configurado intercepta el tráfico SSL y no usa ningún certificado de confianza de otros fabricantes. Si se usa esta opción, se omitirán las comprobaciones incorporadas del certificado, que se utilizan para la sincronización de la garantía y el catálogo.
   d. Haga clic en **Aplicar**.
   e. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para comprender todas las tareas que puede realizar mediante la característica de Configuración de la aplicación, consulte Administración de los ajustes del servidor OpenManage Enterprise en la página 146.

Administración de usuarios de OpenManage Enterprise

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Cualquier cambio en la función de usuario no afectará a la sesión activa de los usuarios afectados y se aplicará en el inicio de sesión subsiguiente.
- Si un usuario del administrador de dispositivos se degrada a Lector, este perderá acceso a todas las entidades de las que es propietario, como trabajos, plantillas de firmware o configuración, bases, políticas de alerta y perfiles. Solo el administrador puede administrar estas entidades y no pueden restaurarse, incluso si el mismo usuario pasa de Lector a DM.

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Usuarios**, puede:

- Ver, agregar, activar, editar, desactivar o eliminar usuarios locales de OpenManage Enterprise. Para obtener más información, consulte Adición y edición de usuarios locales de OpenManage Enterprise.
- Asignar roles de OpenManage Enterprise a los usuarios de Active Directory mediante la importación de los grupos de directorios. A los usuarios del directorio AD y LDAP se les puede asignar una función de Administrador, Administrador de dispositivos o Lector en OpenManage Enterprise. Para obtener más información, consulte Importación de grupos de AD y LDAP en la página 153
- Ver detalles sobre los usuarios conectados y, a continuación, finalizar (cerrar) una sesión de usuario.
- Administrar servicios de directorio. Para obtener más información, consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio en la página 156
- Ver, agregar, activar, editar, desactivar o eliminar proveedores de OpenID Connect (PingFederate o Keycloak). Para obtener más información, consulte Inicio de sesión en OpenManage Enterprise mediante proveedores de OpenID Connect en la página 158

De manera predeterminada, la lista de usuarios se muestra en **Usuarios**. En el panel derecho aparecen las propiedades del nombre de usuario que se selecciona en el panel de trabajo.

- **NOMBRE DE USUARIO**: junto con los usuarios que se hayan creado, OpenManage Enterprise muestra los siguientes roles de usuario predeterminados que no se pueden editar ni eliminar: admin, system y root. Sin embargo, puede editar las credenciales de inicio de sesión; para ello, seleccione el nombre de usuario predeterminado y haga clic en **Editar**. Consulte Activación de usuarios de OpenManage Enterprise en la página 152. Se recomienda utilizar los siguientes caracteres para los nombres de usuario:
  - 0-9
  - A-Z
  - a-z
  - - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >
  - Se recomiendan los siguientes caracteres para contraseñas:
    - 0-9
    - A-Z
    - a-z
    - ' - ! " # $ % & ( ) * , . / : ; ? @ [\ ] ^ _ ` { | } ~ + < = >
- **TIPO DE USUARIO**: indica si los usuarios conectados lo hicieron de forma local o remota.
- **HABILITADO**: indica con una marca de verificación cuando el usuario está habilitado para realizar tareas de administración de OpenManage Enterprise. Consulte Activación de usuarios de OpenManage Enterprise en la página 152 y Desactivación de usuarios de OpenManage Enterprise en la página 153.
- **FUNCIÓN**: indica la función del usuario cuando utiliza OpenManage Enterprise. Por ejemplo, administrador y administrador de dispositivos de OpenManage Enterprise. Consulte Tipos de roles de usuario en OpenManage Enterprise en la página 15.

Referencias relacionadas

Desactivación de usuarios de OpenManage Enterprise en la página 153
Activación de usuarios de OpenManage Enterprise en la página 152

Tareas relacionadas

Eliminación de servicios de directorio en la página 158
Eliminación de usuarios de OpenManage Enterprise en la página 153
Finalización de sesiones de usuario en la página 155

Control de acceso basado en funciones y en el alcance en OpenManage Enterprise

OpenManage Enterprise tiene control de acceso basado en funciones (RBAC), que define claramente los privilegios de usuario para las tres funciones incorporadas: Administrador, Administrador de dispositivos y Lector. Además, mediante el control de acceso basado en el alcance (SBAC), el administrador puede limitar los grupos de dispositivos a los que el administrador de dispositivos tiene acceso. En los siguientes temas, se explican en detalle las funciones RBAC y SBAC.

Privilegios del control de acceso basado en funciones (RBAC) en OpenManage Enterprise

A los usuarios se les asignan funciones que determinan su nivel de acceso a la configuración del dispositivo y a las funciones de administración de dispositivos. Esta función se conoce como Control de acceso basado en funciones (RBAC). La consola exige el privilegio

necesario para una determinada acción antes de permitirla. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte Administración de usuarios de OpenManage Enterprise en la página 147.

En esta tabla, se indican los diversos privilegios activados para cada función.

Tabla 27. Privilegios de usuario basados en roles en OpenManage Enterprise

Funciones de OpenManage Enterprise	Descripción del privilegio	Niveles de usuario para acceder a OpenManage Enterprise		
		Admin (Administrador)	Administrador de dispositivos	Observador
Configuración del dispositivo	Ajustes globales del dispositivo que implican la configuración del dispositivo.	**S**	N	N
Configuración de seguridad	Ajustes de seguridad del dispositivo	**S**	N	N
Administración de alertas	Acciones/administración de alertas	**S**	N	N
Administración de fabric	Acciones/administración de fabric	**S**	N	N
Administración de red	Acciones/administración de red	**S**	N	N
Administración de grupos	Crear, leer, actualizar y eliminar (CRUD) para grupos estáticos y dinámicos	**S**	N	N
Administración de detección	CRUD para tareas de detección, ejecución de tareas de detección	**S**	N	N
Administración de inventario	CRUD para tareas de inventario, ejecución de tareas de inventario	**S**	N	N
Administración de capturas	Importación de MIB, edición de capturas	**S**	N	N
Administración de implementación automática	Administración de operaciones de configuración de implementación automática	**S**	N	N
Configuración de monitoreo	Políticas de alerta, reenvío, SupportAssist etc.	**S**	**S**	N
Control de alimentación	Reinicio o ciclo de energía del dispositivo	**S**	**S**	N
Configuración del dispositivo	Configuración del dispositivo, aplicación de plantillas, administración/migración de identidad de IO, asignación de almacenamiento (para dispositivos de almacenamiento), etc.	**S**	**S**	N
Implementación del sistema operativo	Implementación del sistema operativo, asignación a LUN, etc.	**S**	**S**	N
Actualización del dispositivo	Actualización del firmware del dispositivo, aplicación de bases actualizadas, etc.	**S**	**S**	N
Administración de plantillas	Creación o administración de plantillas	**S**	**S**	N
Administración de base	Creación o administración de políticas de firmware o configuración de base	**S**	**S**	N

Tabla 27. Privilegios de usuario basados en roles en OpenManage Enterprise (continuación)

Funciones de OpenManage Enterprise	Descripción del privilegio	Niveles de usuario para acceder a OpenManage Enterprise		
		Admin (Administrador)	Administrador de dispositivos	Observador
Administración de energía	Establecimiento de asignaciones de energía	**S**	**S**	N
Administración de trabajos	Administración/ejecución de trabajos	**S**	**S**	N
Administración de informes	Operaciones CRUD en informes	**S**	**S**	N
Ejecución de informes	Ejecutar informes	**S**	**S**	**S**
Ver	Visualización de todos los datos, administración o ejecución de informes, etc.	**S**	**S**	**S**

Control de acceso basado en el alcance (SBAC) en OpenManage Enterprise

Con el uso de la función de control de acceso basado en funciones (RBAC), los administradores pueden asignar funciones durante la creación de usuarios. Las funciones determinan el nivel de acceso a los ajustes del dispositivo y a las funciones de administración de dispositivos. El control de acceso basado en el alcance (SBAC) es una extensión de la función de RBAC que permite a un administrador restringir una función de Administrador de dispositivos a un subconjunto de grupos de dispositivos denominado alcance.

Durante la creación o actualización de un usuario con la función Administrador de dispositivos (DM), los administradores pueden asignar un alcance para restringir el acceso operativo del DM a uno o más grupos de sistemas, grupos personalizados o grupos de plug-ins.

Las funciones Administrador y Lector tienen alcance sin restricciones. Esto significa que tienen acceso operativo según lo especificado en los privilegios de RBAC a todas las entidades de dispositivos y grupos.

El alcance puede implementarse de la siguiente manera:

1. Crear o editar usuario
2. Asignar función de DM
3. Asignar el alcance para restringir el acceso operativo

Para obtener más información acerca de la administración de usuarios, consulte Administración de usuarios de OpenManage Enterprise en la página 147.

Cuando un usuario con la función Administrador de dispositivos (DM) y con un alcance asignado inicia sesión, el DM solo puede ver y administrar dispositivos que se encuentren dentro de su alcance. Además, el DM puede ver y administrar entidades, como trabajos, líneas de base y plantillas de firmware o configuración, políticas de alerta, perfiles, etc., que estén asociadas con los dispositivos dentro del alcance, solo si el DM es propietario de la entidad (el DM creó esa entidad o se le asignó la propiedad). Para obtener más información acerca de las entidades que puede crear un DM, consulte *Privilegios de control de acceso basado en funciones (RBAC) en OpenManage Enterprise*.

Por ejemplo, cuando hace clic en **Configuración** > **Plantillas**, un usuario con la función DM puede ver las plantillas predeterminadas y personalizadas que le pertenecen al DM. Además, el DM puede realizar otras tareas si en el RBAC se le otorgan privilegios para las plantillas que le pertenecen.

Si hace clic en **Configuración** > **Pools de identidades**, el DM puede ver todas las identidades que creó un administrador o el DM. El DM también puede realizar acciones en las identidades especificadas por los privilegios de RBAC. Sin embargo, el DM solo puede ver el uso de las identidades que están asociadas a los dispositivos dentro del alcance del DM.

Del mismo modo, si hace clic en **Configuración** > **Pools de VLAN**, el DM puede ver y exportar todas las VLAN que creó el administrador. El DM no puede realizar ninguna otra operación. Si el DM tiene una plantilla, la puede editar para utilizar las redes VLAN, pero no puede editar la red VLAN.

En OpenManage Enterprise, el alcance se puede asignar durante la creación local o importación de un usuario de AD/LDAP. La asignación del alcance a usuarios de OIDC solo se puede realizar en proveedores de Open ID Connect (OIDC).

SBAC para usuarios locales:

Cuando crea o edita un usuario local con la función de DM, el administrador puede seleccionar uno o más grupos de dispositivos que definen el alcance del DM.

Por ejemplo, usted (como administrador) crea un DM llamado dm1 y asigna el grupo *g1* presente en grupos personalizados. Entonces, dm1 solo tendrá acceso operativo a todos los dispositivos en *g1*. El usuario dm1 no podrá acceder a ningún otro grupo o entidad relacionada con otros dispositivos.

Además, con SBAC, dm1 tampoco podrá ver las entidades que cree otro DM (por ejemplo, dm2) en el mismo grupo *g1*. Esto significa que un DM solo podrá ver las entidades que le pertenecen a su usuario.

Por ejemplo, usted (como administrador) crea otro DM llamado dm2 y asigna el mismo grupo *g1* presente en grupos personalizados. Si dm2 crea una plantilla de configuración, líneas de base de configuración o perfiles para los dispositivos en *g1*, el dm1 no tendrá acceso a esas entidades, y viceversa.

Un DM con el alcance Todos los dispositivos tiene acceso operativo según lo especificado en los privilegios de RBAC para todos los dispositivos y las entidades de grupo que le pertenecen al DM.

SBAC para usuarios de AD/LDAP:

Durante la importación o edición de grupos de AD/LDAP, los administradores pueden asignar alcances para grupos de usuarios con la función de DM. Si un usuario es miembro de varios grupos de AD, cada uno con una función de DM, y cada grupo de AD tiene distintas asignaciones de alcance, el alcance del usuario es la combinación de los alcances de esos grupos de AD.

Por ejemplo,

- El usuario dm1 es miembro de dos grupos de AD (*RR5-Floor1-LabAdmins* y *RR5-Floor3-LabAdmins*). Ambos grupos de AD tienen asignada la función de DM, y las asignaciones de alcance para los grupos de AD son las siguientes: *RR5-Floor1-LabAdmins* obtiene *ptlab-servers* y *RR5-Floor3-LabAdmins* obtiene *smdlab-servers*. Ahora, el alcance del DM dm1 es la combinación de *ptlab-servers* y *smdlab-servers*.
- El usuario dm1 es miembro de dos grupos de AD (*adg1* y *adg2*). Ambos grupos de AD tienen asignada la función de DM, con asignaciones de alcance para los grupos de AD como se indica a continuación: *adg1* recibe acceso a *g1* y *adg2* recibe acceso a *g2*. Si *g1* es el supraconjunto de *g2*, el alcance de dm1 es el alcance mayor (*g1*, todos sus grupos secundarios y todos los dispositivos inferiores).

Cuando un usuario es miembro de varios grupos de AD que tienen diferentes funciones, la de mayor funcionalidad tiene prioridad (en el orden Administrador, DM, Lector).

Un DM con acceso sin restricciones tiene acceso operativo según lo especificado en los privilegios de RBAC a todas las entidades de dispositivos y grupos.

NOTA: Después de actualizar OpenManage Enterprise a la versión 3.6, los administradores de dispositivos AD/LDAP y OIDC (PingFederate o KeyCloak) deben volver a crear todas las entidades de la versión anterior, ya que estas entidades solo están disponibles para los administradores después de la actualización. Para obtener más información, consulte las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

SBAC para usuarios de OIDC:

La asignación de alcance para usuarios de OIDC no se realiza en la consola de OME. Puede asignar alcances para usuarios de OIDC en un proveedor de OIDC durante la configuración de usuario. Cuando el usuario inicie sesión con las credenciales del proveedor de OIDC, la asignación de la función y el alcance estará disponible para OME. Para obtener más información acerca de la configuración de las funciones y los alcances de usuario, consulte Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160.

NOTA: Si se utiliza PingFederate como el proveedor de OIDC, solo se pueden usar las funciones de administrador. Para obtener más información, consulte Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160 y las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transferir propiedad: El administrador puede transferir recursos de a un administrador de dispositivos (fuente) a otro administrador de dispositivos. Por ejemplo, un administrador puede transferir todos los recursos asignados del dm1 de fuente al dm2. Un administrador de dispositivos que sea propietario de entidades, como líneas de base de firmware o configuración, plantillas de configuración, políticas de alerta y perfiles, se considera un usuario de fuente elegible. La transferencia de propiedad se realiza solo con las entidades y no los grupos de dispositivos (alcance) que son propiedad de un administrador de dispositivos a otro. Para obtener más información, consulte Transferir la propiedad de entidades de administrador de dispositivos en la página 154.

Referencias relacionadas

Tipos de roles de usuario en OpenManage Enterprise en la página 15

Tareas relacionadas

Instalar OpenManage Enterprise en la página 20

Adición y edición de usuarios locales de OpenManage Enterprise

Este procedimiento es específico solo para agregar o modificar los usuarios locales. Mientras edita los usuarios locales, puede editar todas las propiedades de usuario. Sin embargo, para los usuarios de directorio, solo se pueden editar los grupos de roles y de dispositivos (en caso de un administrador de dispositivos). Para integrar los servicios de directorio en OpenManage Enterprise y para importar los usuarios de directorio, consulte Integración de servicios de directorio en OpenManage Enterprise en la página 155 y Importación de grupos de AD y LDAP en la página 153.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- No se pueden habilitar, deshabilitar ni eliminar los usuarios de admin/sistema/root. Solo puede cambiar la contraseña si hace clic en **Editar** en el panel derecho.

1. Seleccione **Ajustes de la aplicación** > **Usuarios** > **Usuarios** > **Agregar**.
2. En el cuadro de diálogo **Agregar nuevo usuario**:
   a. En **Detalles del usuario**, seleccione Administrador, Administrador de dispositivos u Observador en el menú desplegable **Rol del usuario**.

      Para obtener más información, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

      De manera predeterminada, la casilla de verificación **Activado** está seleccionada para indicar que los privilegios de usuario que se están configurando están habilitados para un usuario.

   b. En el caso de los roles de administrador de dispositivos, el alcance se establece de manera predeterminada en **Todos los dispositivos** (alcance sin restricciones); sin embargo, el administrador puede restringir el alcance al elegir la opción **Seleccionar grupos**, seguido de la selección de los grupos de dispositivos.
   c. En **Información de identificación**, ingrese el **nombre de usuario**, la **contraseña** y vuelva a ingresar la contraseña en los campos **Confirmar contraseña**.

      NOTA: El nombre de usuario debe contener solo caracteres alfanuméricos (pero se permite guion bajo) y la contraseña debe contener al menos un carácter en mayúscula, un carácter en minúscula, un dígito y un carácter especial.

3. Haga clic en **Finalizar**.
   De este modo, aparece un mensaje que indica que el usuario se guardó correctamente. Se inicia un trabajo para crear un nuevo usuario. Después de ejecutar el trabajo, el nuevo usuario se crea y se muestra en la lista de usuarios.

Edición de propiedades de usuario de OpenManage Enterprise

1. En la página **Configuración de la aplicación**, en **Usuarios**, seleccione la casilla de verificación que corresponde al usuario.
2. Realice las tareas en Adición y edición de usuarios locales de OpenManage Enterprise en la página 152.
   Los datos actualizados se guardan.

   NOTA: Cuando cambia el rol de un usuario, los privilegios disponibles para el rol nuevo se aplican automáticamente. Por ejemplo, si cambia un administrador de dispositivos a administrador, los derechos y privilegios de acceso que se proporcionan a un administrador se activan automáticamente para el administrador de dispositivos.

Activación de usuarios de OpenManage Enterprise

Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Habilitar**. Si el usuario está habilitado, la marca visto desaparecerá de la celda correspondiente de la columna **HABILITADO**. Si el usuario ya se encuentra habilitado durante la creación del nombre de usuario, el botón **Habilitar** se muestra atenuado.

Tareas relacionadas

Eliminación de servicios de directorio en la página 158
Eliminación de usuarios de OpenManage Enterprise en la página 153
Finalización de sesiones de usuario en la página 155

Información relacionada

Administración de usuarios de OpenManage Enterprise en la página 147

Desactivación de usuarios de OpenManage Enterprise

Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Deshabilitar**. El usuario está deshabilitado y una marca visto desaparece en la celda correspondiente de la columna **HABILITADO**. Si el usuario está deshabilitado cuando se crea el nombre de usuario, el botón **Deshabilitar** se muestra atenuado.

Tareas relacionadas

Eliminación de servicios de directorio en la página 158
Eliminación de usuarios de OpenManage Enterprise en la página 153
Finalización de sesiones de usuario en la página 155

Información relacionada

Administración de usuarios de OpenManage Enterprise en la página 147

Eliminación de usuarios de OpenManage Enterprise

1. Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Eliminar**.
2. Cuando se le solicite, haga clic en **SÍ**.

Referencias relacionadas

Desactivación de usuarios de OpenManage Enterprise en la página 153
Activación de usuarios de OpenManage Enterprise en la página 152

Información relacionada

Administración de usuarios de OpenManage Enterprise en la página 147

Importación de grupos de AD y LDAP

NOTA:

- Los usuarios sin derechos de administrador no pueden activar ni desactivar usuarios de Active Directory (AD) ni de protocolo ligero de acceso a directorios (LDAP).
- Antes de importar grupos de AD en OpenManage Enterprise, debe incluir los grupos de usuarios en un GRUPO UNIVERSAL mientras configura el AD.
- Los usuarios del directorio AD y LDAP pueden importarse y se les puede asignar uno de los roles de OpenManage Enterprise (administrador, administrador de dispositivos o visor). La función de inicio de sesión único (SSO) detiene el inicio de sesión en la consola. Las acciones que se ejecutan en los dispositivos requieren una cuenta con privilegios en el dispositivo.
- Después de actualizar OpenManage Enterprise a la versión 3.6, los administradores de dispositivos AD/LDAP y OIDC (PingFederate o KeyCloak) deben volver a crear todas las entidades de la versión anterior, ya que estas entidades solo están disponibles para los administradores después de la actualización. Para obtener más información, consulte las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

1. Haga clic en **Importar grupo de directorio**.
2. En el cuadro de diálogo **Importar Active Directory**:
   a. En el menú desplegable **Origen de directorio**, seleccione un origen de AD o LDAP que se deba importar para agregar grupos. Para agregar directorios, consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio en la página 156.
   b. Haga clic en **Ingresar credenciales**.

c. En el cuadro de diálogo, ingrese el nombre de usuario y la contraseña del dominio en el que se guarda el directorio. Utilice la información sobre herramientas para ingresar la sintaxis correcta.
d. Haga clic en **Finalizar**.

3. En la sección **Grupos disponibles**:
   a. En la casilla **Buscar un grupo**, ingrese algunas letras iniciales del nombre del grupo disponible en el directorio probado. Todos los nombres de grupos que comiencen con el texto ingresado aparecen en el NOMBRE DE GRUPO.
   b. Seleccione las casillas de verificación correspondientes a los grupos que se deban importar y, a continuación, haga clic en los botones **>> o <<** para agregar o quitar los grupos.
4. En la sección **Grupos que se deban importar**:
   a. Seleccione las casillas de verificación de los grupos y, a continuación, seleccione una función del menú desplegable Asignar rol de grupo. Para obtener más información sobre el acceso basado en el rol, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
   b. Haga clic en **Asignar función**.
   Los usuarios de un grupo en el servicio de directorio seleccionado se asignan con las funciones del usuario seleccionado.
   c. En el caso de la función Administrador de dispositivos, el alcance se establece de manera predeterminada en **Todos los dispositivos**; sin embargo, el administrador puede restringir el alcance si selecciona la opción **Asignar alcance** y, luego, selecciona grupos de dispositivos.
5. Repita los pasos 3 y 4, si fuera necesario.
6. Haga clic en **Importar**.
   Los grupos de directorios se importan y se muestran en la lista de usuarios. Sin embargo, todos los usuarios de esos grupos iniciarán sesión en OpenManage Enterprise con sus credenciales y nombres de usuario de dominio.

Es posible que un usuario de dominio, por ejemplo john_smith, sea miembro de varios grupos de directorios y que también para esos grupos se le asignen distintos roles. En este caso, se muestran varias funciones, como Administrador de dispositivos y Lector, tras desplazar el cursor sobre el nombre de usuario en la esquina derecha de la cabecera del dispositivo. Tales usuarios recibirán la función de mayor nivel para todos los grupos de directorios de los que el usuario es miembro.

- Ejemplo 1: el usuario es miembro de los tres grupos con roles de admin, DM y observador. En este caso, el usuario se convierte en administrador.
- Ejemplo 2: el usuario es miembro de tres grupos de DM y un grupo de observadores. En este caso, el usuario se convertirá en el DM con acceso a la unión de grupos de dispositivos en los tres roles de DM.

Transferir la propiedad de entidades de administrador de dispositivos

En este tema, se describe la forma en que un administrador puede transferir entidades, como trabajos, plantillas de firmware o configuración y líneas de base, políticas de alerta y perfiles que creó un administrador de dispositivos a otro administrador de dispositivos. El administrador puede iniciar una "transferencia de propiedad" cuando un administrador de dispositivos deja la organización.

NOTA:

- Para realizar esta tarea en OpenManage Enterprise, debe tener los privilegios de usuario administrador. Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- La "transferencia de propiedad" se realiza solo con las entidades y no los grupos de dispositivos (alcance) que son propiedad de un administrador de dispositivos a otro.
- Antes de que se inicie la transferencia de propiedad de entidades, el administrador primero debe reasignar los grupos de dispositivos que le pertenecen al administrador de dispositivos anterior al administrador de dispositivos que tomará el control.
- Si la propiedad de las entidades se transfiere a un grupo de usuarios de Active Directory, esta propiedad se transfiere a todos los miembros de ese grupo de AD.

Para transferir la propiedad de las entidades, como trabajos, líneas de base y plantillas de firmware o configuración, políticas de alerta y perfiles de un administrador de dispositivos a otro, haga lo siguiente:

1. Para iniciar el asistente Transferir propiedad, haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Usuarios** > **Transferir propiedad**.
2. En la lista desplegable **Usuario de fuente**, seleccione el administrador de dispositivos desde el que se debe transferir la propiedad de las entidades.

   NOTA: El usuario de fuente solo mostrará la lista de administradores de dispositivos locales, de Active Directory, OIDC o eliminados, que tengan entidades como trabajos, plantillas de FW o configuración, políticas y perfiles de alertas asociados con ellos.

3. En la lista desplegable **Usuario objetivo**, seleccione el administrador de dispositivos al que se debe transferir la propiedad de las entidades.

4. Haga clic en **Finalizar** y, luego, haga clic en **Sí** en el mensaje de solicitud.

Todas las entidades que le pertenecen, como los trabajos, las plantillas de firmware o de configuración, las políticas de alerta y los perfiles, se transfieren desde el administrador de dispositivos fuente al administrador de dispositivos objetivo.

Finalización de sesiones de usuario

1. Seleccione la casilla de verificación correspondiente al nombre de usuario y, luego, haga clic en **Finalizar**.
2. Cuando se le solicite confirmación, haga clic en **SÍ**.
   La sesión de usuario seleccionada termina y se cierra la sesión del usuario.

Referencias relacionadas

Desactivación de usuarios de OpenManage Enterprise en la página 153
Activación de usuarios de OpenManage Enterprise en la página 152

Información relacionada

Administración de usuarios de OpenManage Enterprise en la página 147

Integración de servicios de directorio en OpenManage Enterprise

Los servicios de directorio permiten importar grupos de directorios desde AD o LDAP para su uso en la consola. OpenManage Enterprise es compatible con la integración de los siguientes servicios de directorio:

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP con LDAP

Requisitos previos/atributos admitidos para la integración de LDAP

Tabla 28. Requisitos previos/atributos admitidos de OpenManage Enterprise para la integración de LDAP

	Atributo de inicio de sesión del usuario	Atributo de pertenencia a grupos	Requisito de certificado
AD/LDAP	Cn, sAMAccountName	Miembro	• Debe tener FQSN y está sujeto a las necesidades de certificado de controladora de dominio. El campo SAN puede tener IPv4, IPv6 o FQDN. • Solo se admite el formato de certificado Base64
OpenLDAP	uid, sn	Uniquemember	Solo se admite el formato de certificado PEM
PHP con LDAP	uid	MemberUid	

Requisitos previos de usuario para la integración del servicio de directorio

Debe asegurarse de que se cumplan los siguientes requisitos previos de usuario antes de comenzar con la integración del servicio de directorio:

1. El usuario BindDN y el usuario que se usa para “probar la conexión” deben ser los mismos.
2. Si se proporciona el atributo de inicio de sesión del usuario, se permite solo el valor de nombre de usuario correspondiente asignado al atributo para iniciar sesión en el dispositivo.

3. El usuario que se utiliza para la prueba de conexión debe formar parte de algún grupo no predeterminado de LDAP
4. El atributo de membresía de grupo debe contener el "userDN" o el nombre corto (utilizado para iniciar sesión) del usuario.
5. Cuando MemberUid se utiliza como "atributo de membresía de grupo", se considerará que el nombre de usuario utilizado en el inicio de sesión de dispositivos distingue mayúsculas de minúsculas en algunas configuraciones de LDAP.
6. Cuando el filtro de búsqueda se usa en la configuración de LDAP, el inicio de sesión del usuario no se permite para aquellos usuarios que no forman parte de los criterios de búsqueda mencionados.
7. La búsqueda de grupos funcionará solo si los grupos tienen usuarios asignados en el atributo de membresía de grupo proporcionado.

NOTA: Si OpenManage Enterprise está alojado en una red IPv6, la autenticación SSL en relación con la controladora de dominio que usa el FQDN fallaría si IPv4 se establece como dirección preferida en el DNS. Para evitar este error, realice una de las siguientes acciones:

- DNS debe configurarse para arrojar IPv6 como dirección preferida cuando se consulta con FQDN.
- El certificado DC debe tener IPv6 en el campo SAN.

Para utilizar los servicios de directorio:

- Agregue una conexión de directorios. Consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio en la página 156.
- Importe grupos de directorio y asigne todos los usuarios en el grupo para un rol específico. Consulte Importación de grupos de AD y LDAP en la página 153.
- Para usuarios DM, edite el grupo de directorio para agregar los grupos que el DM puede administrar. Consulte Adición y edición de usuarios locales de OpenManage Enterprise en la página 152.

Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio

1. Haga clic en **Configuración de la aplicación** > **Usuarios** > **Servicios de directorio** y luego en **Agregar**.
2. En el cuadro de diálogo **Conectarse al servicio de directorio**, de forma predeterminada, se selecciona **AD** para indicar que el tipo de directorio es Active Directory (AD):

   NOTA: Para crear un grupo de usuarios de LDAP mediante Servicios de directorio, consulte Adición o edición de grupos de LDAP que se utilizarán con los Servicios de directorio en la página 157.

   a. Ingrese un nombre de su preferencia para el directorio de AD.
   b. Seleccione el método de búsqueda de las controladoras de dominio:
      - **DNS**: en la casilla **Método**, escriba el nombre del dominio a fin de consultar DNS para las controladoras de dominio.
      - **Manual**: en la casilla **Método**, ingrese la dirección IP o el FQDN de la controladora de dominio. En lo que respecta a varios servidores, se admite un máximo de tres servidores y se debe utilizar una lista separada por comas.
   c. En la casilla **Dominio del grupo**, ingrese el dominio del grupo como se sugiere en la sintaxis de la información sobre herramientas.
3. En la sección **Opciones avanzadas**:
   a. De manera predeterminada, el número de puerto de la dirección del catálogo global se llena con 3269. Para el acceso a la controladora de dominio, escriba 636 como el número de puerto.

      NOTA: Solo se admiten puertos LDAPS.

   b. Escriba la duración del tiempo de espera de red y del tiempo de espera de búsqueda en segundos. La duración del tiempo de espera máximo admitido es de 300 segundos.
   c. Para cargar un certificado SSL, seleccione **Validación del certificado** y haga clic en **Seleccionar un archivo**. El certificado deberá ser un certificado de CA raíz codificado en formato Base64.

   Se muestra la pestaña **Probar conexión**.
4. Haga clic en **Probar conexión**.
5. En el cuadro de diálogo, ingrese el **nombre de usuario** y la **contraseña** del dominio al que se debe conectar.

   NOTA: El **nombre de usuario** se debe ingresar en el UPN (nombredeusuario@dominio) o en el formato (dominio\nombre) de NetBIOS.
6. Haga clic en **Probar conexión**.
   En el cuadro de diálogo **Información de servicio de directorio**, se muestra un mensaje para indicar que la conexión es satisfactoria.

7. Haga clic en **Ok**.
8. Haga clic en **Finalizar**.
   Se crea y ejecuta un trabajo para agregar el directorio solicitado en la lista de servicios de directorio.

1. En la columna **NOMBRE DE DIRECTORIO**, seleccione el directorio. En el panel derecho se muestran las propiedades del servicio de directorio.
2. Haga clic en **Editar**.
3. En el cuadro de diálogo **Conectarse al servicio de directorio**, edite los datos y haga clic en **Finalizar**. Los datos se actualizan y se guardan.

Adición o edición de grupos de LDAP que se utilizarán con los Servicios de directorio

1. Haga clic en **Configuración de la aplicación** > **Usuarios** > **Servicios de directorio** y luego en **Agregar**.
2. En el cuadro de diálogo **Conectarse al servicio de directorio**, seleccione **LDAP** como el tipo de directorio.

   NOTA: Para crear un grupo de usuarios de AD mediante Servicios de directorio, consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio en la página 156.

   a. Ingrese un nombre de su preferencia para el directorio LDAP.
   b. Seleccione el método de búsqueda de las controladoras de dominio:
      - **DNS**: en la casilla **Método**, escriba el nombre del dominio a fin de consultar DNS para las controladoras de dominio.
      - **Manual**: en la casilla **Método**, ingrese la dirección IP o el FQDN de la controladora de dominio. En lo que respecta a varios servidores, se admite un máximo de tres servidores y se debe utilizar una lista separada por comas.
   c. Ingrese el nombre distinguido (DN) de enlace y la contraseña de la carpeta LDAP.

      NOTA: No admite el enlace anónimo para LDS de AD.

3. En la sección **Opciones avanzadas**:
   a. De manera predeterminada, el número de puerto de LDAP se completa con 636. Para cambiarlo, escriba un número de puerto.

      NOTA: Solo se admiten puertos LDAPS.

   b. Para que coincida la configuración de LDAP en el servidor, escriba el DN de la base del grupo que desea buscar.
   c. Ingrese los **Atributos del usuario** ya configurados en el sistema LDAP. Se recomienda que este nombre sea único dentro del DN base seleccionado. De lo contrario, configure un filtro de búsqueda para garantizar que sea único. Si el DN del usuario no se puede identificar únicamente mediante una búsqueda que combine el atributo y el filtro de búsqueda, falla el inicio de sesión.

      NOTA: Antes de integrarlos en los servicios de directorio, los atributos del usuario deben estar configurados en el sistema LDAP que se usa para consultar.

      NOTA: Debe ingresar los atributos del usuario como **cn**o **sAMAccountName** para la configuración de LDS de AD y **UID** para la configuración de LDAP

   d. En el **Atributo de pertenencia a grupos** ingrese el atributo que almacena la información de los grupos y los miembros en el directorio.
   e. Escriba la duración del tiempo de espera de red y del tiempo de espera de búsqueda en segundos. La duración del tiempo de espera máximo admitido es de 300 segundos.
   f. Para cargar un certificado SSL, seleccione **Validación del certificado** y haga clic en **Seleccionar un archivo** El certificado deberá ser un certificado de CA raíz codificado en formato Base64.

   El botón **Probar conexión** está activado.
4. Haga clic en **Probar conexión** y, a continuación, ingrese los parámetros de conexión del usuario de enlace del dominio al que desea conectarse.

   NOTA: Mientras se prueba la conexión, asegúrese de que **Probar nombre** tenga el valor del **Atributo de inicio de sesión del usuario** especificado previamente.
5. Haga clic en **Probar conexión**.
   En el cuadro de diálogo **Información de servicio de directorio**, se muestra un mensaje para indicar que la conexión es satisfactoria.
6. Haga clic en **Aceptar**.
7. Haga clic en **Finalizar**.

Se crea y ejecuta un trabajo para agregar el directorio solicitado en la lista de servicios de directorio.

1. En la columna **NOMBRE DE DIRECTORIO**, seleccione el directorio. En el panel derecho se muestran las propiedades del servicio de directorio.
2. Haga clic en **Editar**.
3. En el cuadro de diálogo **Conectarse al servicio de directorio**, edite los datos y haga clic en **Finalizar**. Los datos se actualizan y se guardan.

Eliminación de servicios de directorio

Seleccione la casilla de verificación correspondiente a los servicios de directorio que se deben eliminar y, a continuación, haga clic en **Eliminar**.

Referencias relacionadas

Desactivación de usuarios de OpenManage Enterprise en la página 153
Activación de usuarios de OpenManage Enterprise en la página 152

Información relacionada

Administración de los ajustes del servidor OpenManage Enterprise en la página 146
Administración de usuarios de OpenManage Enterprise en la página 147

Inicio de sesión en OpenManage Enterprise mediante proveedores de OpenID Connect

Puede iniciar sesión con los proveedores de OpenID Connect (OIDC). Los proveedores de OpenID Connect corresponden al software de administración de usuarios e identidades que permite a los usuarios acceder a las aplicaciones de manera segura. Actualmente, OpenManage Enterprise proporciona soporte para PingFederate y Keycloak.

AVISO: Las funciones y los alcances de los usuarios aparecen restablecidos en "predeterminado" en el nuevo registro del cliente con el proveedor de OIDC PingFederate (PingIdentity). Este problema podría provocar el restablecimiento de los privilegios y el alcance de las funciones no administrativas (DM y Lector) correspondientes al administrador. El nuevo registro de la consola del dispositivo con el proveedor de OIDC se activa en caso de que se produzca una actualización del dispositivo, un cambio en la configuración de la red o un cambio en el certificado SSL.

Para evitar problemas de seguridad después de cualquiera de los eventos de nuevo registro mencionados anteriormente, el administrador debe volver a configurar todos los ID de cliente de OpenManage Enterprise en el sitio de PingFederate. Además, se recomienda encarecidamente que los ID de cliente se creen solo para los usuarios administradores con PingFederate hasta que se resuelva este problema.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.
- Solo se puede agregar un máximo de cuatro ID de proveedores de OpenID Connect en el dispositivo.
- Después de actualizar OpenManage Enterprise a la versión 3.6, los administradores de dispositivos AD/LDAP y OIDC (PingFederate o KeyCloak) deben volver a crear todas las entidades de la versión anterior, ya que estas entidades solo están disponibles para los administradores después de la actualización. Para obtener más información, consulte las notas de la versión en https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs

Requisitos previos:

Antes de habilitar un inicio de sesión del proveedor de OpenID Connect, debe:

1. **Agregar un proveedor de OIDC en OpenManage Enterprise**: en Configuración de la aplicación de OpenManage Enterprise, agregue un proveedor de OpenID Connect. Cuando se agrega el proveedor de OpenID Connect, se genera un **ID de cliente** para el proveedor de OpenID Connect. Para obtener más información, consulte Agregar un proveedor de OpenID Connect a OpenManage Enterprise en la página 159.

2. **Configure el proveedor de OpenID Connect mediante el ID de cliente**: en el proveedor de OpenID Connect, ubique el ID de cliente y defina una función de inicio de sesión (Administrador, Administrador de dispositivos o Visualizador) mediante la adición y la asignación del alcance denominado **dxcua** (reclamación extendida de Dell para la autenticación de usuarios). Para obtener más información, ver:
   - Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160
   - Configuración de una política de proveedor de OpenID Connect en Keycloak para el acceso basado en funciones a OpenManage Enterprise en la página 160

Cuando se agrega un proveedor de OpenID Connect en OpenManage Enterprise, aparece en la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**. Se muestran los siguientes detalles del proveedor de OIDC:

- Nombre: nombre del proveedor de OpenID Connect cuando se agregó en el dispositivo
- Habilitado: una "marca de verificación" en este campo indica que el proveedor de OpenID Connect está habilitado en el dispositivo
- URI de detección: el URI (identificador de recursos uniforme) del proveedor de OpenID Connect
- Estado del registro: puede ser una de las siguientes opciones:
  - Exitoso: indica un registro exitoso con el proveedor de OpenID Connect
  - Fallido: indica un registro fallido con el proveedor de OpenID Connect. El registro "Fallido" del proveedor de OpenID Connect no se podrá realizar incluso cuando esté habilitado.
  - En curso: este estado se muestra cuando el dispositivo intenta registrar el proveedor de OpenID Connect.

En el panel derecho, se muestran el ID de cliente, el estado del registro, el URI de detección del proveedor de OpenID Connect seleccionado. Puede hacer clic en **Ver detalles** para ver los detalles del certificado del proveedor de OpenID Connect.

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, puede realizar las siguientes acciones:

- Agregar un proveedor de OpenID Connect a OpenManage Enterprise en la página 159
- Cómo editar los detalles de un proveedor de OpenID Connect en OpenManage Enterprise en la página 161
- Probar el estado de registro de OpenManage Enterprise con el proveedor de OpenID Connect en la página 161
- Cómo habilitar proveedores de OpenID Connect en la página 161
- Cómo deshabilitar proveedores de OpenID Connect en la página 162
- Cómo eliminar proveedores de OpenID Connect en la página 162

Agregar un proveedor de OpenID Connect a OpenManage Enterprise

La incorporación, la habilitación y el registro de un proveedor de OpenID Connect (Keycloak o PingFederate) permiten que un cliente autorizado inicie sesión en OpenManage Enterprise. De esta manera, se genera un ID de cliente.

Para agregar un proveedor de OpenID Connect a OpenManage Enterprise, vaya a la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect** y realice las siguientes acciones:

NOTA: Solo se puede agregar un máximo de cuatro clientes al proveedor de OpenID Connect.

1. Haga clic en **Agregar** para activar la página Agregar nuevo proveedor de OpenID Connect.
2. Proporcione la siguiente información en los campos correspondientes:
   a. Nombre: nombre del cliente de OIDC.
   b. URI de detección: identificador de recursos uniforme del proveedor de OIDC
   c. Tipo de autenticación: seleccione uno de los siguientes métodos que el token de acceso debe usar para acceder al dispositivo:
      i. Token de acceso inicial: proporcione el token de acceso inicial
      ii. Nombre de usuario y contraseña: proporcione el nombre de usuario y la contraseña
   d. (Opcional) Casilla de verificación Certificar validación: puede marcar la casilla de verificación y cargar el certificado del proveedor de OIDC haciendo clic en **Examinar** y localizando el certificado o arrastrando y soltando el certificado en el cuadro "línea discontinua".
   e. (Opcional) Probar conexión: haga clic en **Probar URI y conexión SSL** para probar la conexión con el proveedor de OpenID Connect.
      NOTA: La conexión de prueba no depende del nombre de usuario y la contraseña ni de los detalles de tokens de acceso iniciales, ya que solo comprueba la validez del URI de detección proporcionado.
   f. (Opcional) Casilla de verificación Habilitado: puede marcar la casilla de verificación para permitir que los tokens de acceso de clientes autorizados inicien sesión en el dispositivo.
3. Haga clic en **Finalizar**.

El proveedor OpenID Connect recién agregado aparece en la página Configuración de la aplicación > Usuarios > Proveedores de OpenID Connect y el ID del cliente se puede encontrar en el panel derecho.

Próximos pasos:

Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise en la página 160

Configuración de una política de proveedor de OpenID Connect en Keycloak para el acceso basado en funciones a OpenManage Enterprise en la página 160

Configuración de una política de proveedor de OpenID Connect en PingFederate para el acceso basado en funciones a OpenManage Enterprise

Para habilitar el inicio de sesión en OpenManage Enterprise OpenID Connect mediante PingFederate, primero debe agregar y asignar un alcance **dxcua** (reclamación extendida de Dell para la autenticación de usuarios) para el ID de cliente y definir los privilegios de usuarios de la siguiente manera:

AVISO: Las funciones y los alcances de los usuarios aparecen restablecidos en "predeterminado" en el nuevo registro del cliente con el proveedor de OIDC PingFederate (PingIdentity). Este problema podría provocar el restablecimiento de los privilegios y el alcance de las funciones no administrativas (DM y Lector) correspondientes al administrador. El nuevo registro de la consola del dispositivo con el proveedor de OIDC se activa en caso de que se produzca una actualización del dispositivo, un cambio en la configuración de la red o un cambio en el certificado SSL.

Para evitar problemas de seguridad después de cualquiera de los eventos de nuevo registro mencionados anteriormente, el administrador debe volver a configurar todos los ID de cliente de OpenManage Enterprise en el sitio de PingFederate. Además, se recomienda encarecidamente que los ID de cliente se creen solo para los usuarios administradores con PingFederate hasta que se resuelva este problema.

NOTA:

- El algoritmo de asignación predeterminado debe ser RS256 (firma RSA con SHA-256).

1. Agregue un alcance "exclusivo" o "predeterminado" denominado **dxcua** en Administración de alcance en Configuración de OAuth.
2. Asigne el alcance creado en **Administración de políticas de OpenID Connect** > **Política** con los siguientes pasos:
   a. Habilite **Incluir información de usuario en el token**
   b. En Alcance del atributo, agregue el valor para el alcance y el valor **dxcua**.
   c. En Cumplimiento de contrato, agregue dxcua y seleccione el tipo como "texto". Luego, defina los privilegios de usuario para el inicio de sesión del proveedor de OpenManage Enterprise OpenID Connect mediante uno de los siguientes atributos:
      i. Administrador: `dxcua : [{"Role": "AD"}]`
      ii. Administrador de dispositivos: `dxcua : [{"Role": "DM"}]`
      NOTA: Para restringir el acceso del administrador de dispositivos a determinados grupos de dispositivos, por ejemplo, G1 y G2, en OpenManage Enterprise, use `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
      iii. Visualizador: `dxcua : [{"Role": "VE"}]`
   d. Si se configura un alcance "exclusivo" después del registro del cliente en OpenManage Enterprise, edite el cliente configurado en PingFederate y habilite el alcance exclusivo y creado "dxcua".
3. El **registro dinámico de clientes** debe estar habilitado en PingFederate para el registro de clientes de OpenManage Enterprise. Si la opción "Requerir token de acceso inicial" no está marcada en la configuración del cliente del proveedor de OpenID Connect, el registro utilizará el nombre de usuario y la contraseña. Si la opción está habilitada, el registro utilizará únicamente el token de acceso inicial.

Configuración de una política de proveedor de OpenID Connect en Keycloak para el acceso basado en funciones a OpenManage Enterprise

Para habilitar el inicio de sesión en OpenManage Enterprise OpenID Connect mediante Keycloak, primero debe agregar y asignar un alcance **dxcua** para el ID de cliente y definir los privilegios de usuarios de la siguiente manera:

NOTA: El URI de detección especificado en el asistente de configuración del proveedor de OpenID Connect debe tener una terminal válida del proveedor indicado.

1. En la sección Atributos de Usuarios de Keycloak, defina la "clave" y el "valor" para las funciones de inicio de sesión en OpenManage Enterprise mediante uno de los siguientes atributos:
   - Administrador: `dxcua : [{"Role": "AD"}]`
   - Administrador de dispositivos: `dxcua : [{"Role": "DM"}]`

     NOTA: Para restringir el acceso del administrador de dispositivos a determinados grupos de dispositivos, por ejemplo, G1 y G2, en OpenManage Enterprise, use `dxcua : [{"Role": "DM", "Entity":"G1, G2"}]`
   - Visualizador: `dxcua : [{"Role": "VE"}]`
2. Una vez que el cliente esté registrado en Keycloak, en la sección Asignadores, agregue un tipo de asignador "Atributo de usuario" con los siguientes valores:
   - Nombre: dxcua
   - Tipo de asignador: atributo de usuario
   - Atributo de usuario: dxcua
   - Nombre de reclamación de token: dxcua
   - Tipo Json de reclamación: cadena
   - Agregar a token de ID: habilitar
   - Agregar a token de acceso: habilitar
   - Agregar a información de usuario: habilitar

Probar el estado de registro de OpenManage Enterprise con el proveedor de OpenID Connect

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, realice las siguientes acciones:

1. Seleccione un proveedor de OpenID Connect.
2. En el panel derecho, haga clic en **Probar estado de registro**.

   NOTA: La conexión de prueba no depende del nombre de usuario y la contraseña ni de los detalles de tokens de acceso iniciales, ya que solo comprueba la validez del URI de detección.

Se actualizó el estado de registro más reciente ("correcto" o "fallido") con el proveedor de OIDC.

Cómo editar los detalles de un proveedor de OpenID Connect en OpenManage Enterprise

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, realice las siguientes acciones:

1. Seleccione un proveedor de OpenID Connect.
2. Haga clic en **Editar** en el panel derecho.
3. Según el estado del registro del cliente del proveedor de OpenID Connect, puede realizar las siguientes acciones:
   a. Si el estado del registro es "Exitoso", solo se pueden editar las casillas de verificación Validación de certificación, Probar conexión y Habilitado.
   b. Si el estado del registro es "Fallido", puede editar las casillas de verificación Nombre de usuario, Contraseña, Validación de certificación, Probar conexión y Habilitado.
4. Haga clic en **Finalizar** para implementar o en **Cancelar** para descartar los cambios.

Cómo habilitar proveedores de OpenID Connect

Si el inicio de sesión de un proveedor de OpenID Connect no estaba habilitado en el momento en que se agregó al dispositivo, para activar el inicio de sesión debe "habilitarlo" en el dispositivo.

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, realice las siguientes acciones:

1. Seleccione los proveedores de OpenID Connect.
2. Haga clic en **Habilitar**.

La habilitación de los proveedores de OpenID Connect en OpenManage Enterprise permite a los tokens de acceso de clientes autorizados iniciar sesión en el dispositivo.

Cómo eliminar proveedores de OpenID Connect

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, realice las siguientes acciones:

1. Seleccione los proveedores de OpenID Connect.
2. Haga clic en **Eliminar**.

Cómo deshabilitar proveedores de OpenID Connect

En la página **Configuración de la aplicación** > **Usuarios** > **Proveedores de OpenID Connect**, realice las siguientes acciones:

1. Seleccione los proveedores de OpenID Connect.
2. Haga clic en **Deshabilitar**.

El token de acceso del cliente de los proveedores de OIDC "deshabilitados" será rechazado por el dispositivo.

Certificados de seguridad

Si hace clic en **Configuración de la aplicación SeguridadCertificados**, puede ver la información sobre el certificado SSL actualmente disponible para el dispositivo.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Para generar una solicitud de firma de certificado (CSR), consulte Generación y descarga de la solicitud de firma de certificado en la página 162.

Generación y descarga de la solicitud de firma de certificado

Para generar una solicitud de firma de certificado (CSR) para su dispositivo y, a continuación, solicitar un certificado SSL:

NOTA: Solo debe generar la CSR en el dispositivo OpenManage Enterprise.

1. Haga clic en **Generar una solicitud de firma de certificado**.
2. En el cuadro de diálogo **Generar solicitud de firma de certificado**, ingrese información en los campos.
3. Haga clic en **Generar**.
   Una CSR se crea y se muestra en el cuadro de diálogo **Solicitud de firma de certificado**. Una copia de la CSR también se envía a la dirección de correo electrónico que se proporciona en la solicitud.
4. En el cuadro de diálogo **Solicitud de firma de certificado**, copie los datos de la CSR y envíela a la autoridad emisora de certificados (CA) mientras se solicita un certificado SSL.
   - Para descargar la CSR, haga clic en **Descargar solicitud de firma de certificado**.
   - Haga clic en **Finalizar**.

Asignar un certificado de servidor web a OpenManage Enterprise mediante los servicios de certificados de Microsoft

1. Generar y descargar la solicitud de firma de certificado (CSR) en OpenManage Enterprise. Consulte Generación y descarga de la solicitud de firma de certificado en la página 162
2. Abra una sesión web en el servidor de certificación (https://x.x.x.x/certsrv) y haga clic en el enlace **Solicitar un certificado**.
3. En la página Solicitar un certificado, haga clic en el enlace **Enviar una solicitud avanzada de certificado**.
4. En la página Solicitud avanzada de certificado, haga clic en el enlace **Enviar una solicitud de certificado mediante un archivo CMC o PKCS#10 codificado de base 64 o enviar una solicitud de renovación mediante un archivo PKCS#7 codificado de base 64**.
5. En la página Enviar una solicitud de certificado o de renovación, realice lo siguiente:
   a. En el campo **Solicitud de certificado codificado de base 64 (archivo CMC, PKCS#10 o PKCS#7)**, copie y pegue todo el contenido de la CSR descargada.

b. En **Plantilla de certificado**, seleccione **Servidor web**.
c. Haga clic en **Enviar** para emitir un certificado.

6. En la página Certificado emitido, seleccione la opción **Codificado de base 64** y, luego, haga clic en el enlace **Descargar certificado** para descargar el certificado.
7. Para cargar el certificado en OpenManage, vaya a la página **Configuración de aplicación** > **Seguridad** > **Certificados** y, luego, hacer clic en **Cargar**.

Establecimiento de las propiedades de seguridad de inicio de sesión

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

NOTA: Los usuarios del directorio AD y LDAP pueden importarse y se les puede asignar uno de los roles de OpenManage Enterprise (administrador, administrador de dispositivos o visor).

Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Seguridad** para proteger OpenManage Enterprise especificando la opción **Restringir rango de IP permitido** o **Política de bloqueo de inicio de sesión**.

- Expanda **Restringir rango de IP permitido**:
  NOTA: Cuando la opción "Restringir rango de IP permitido" está configurada en un dispositivo, cualquier conexión entrante al dispositivo, como la recepción de alertas, las actualizaciones de firmware y las identidades de red se bloquea para los dispositivos que no se encuentran dentro del rango determinado. Sin embargo, cualquier conexión que salga del dispositivo funcionará en todos los dispositivos.
  1. Para especificar el rango de direcciones IP que deben tener permiso para acceder a OpenManage Enterprise, seleccione la casilla de verificación **Activar rango de IP**.
  2. En la casilla **Dirección de rango IP (CIDR)**, ingrese el rango de direcciones IP.
     NOTA: Solo se permite un rango de IP.
  3. Haga clic en **Aplicar**. Para restablecer las propiedades predeterminadas, haga clic en **Descartar**.
     NOTA: El botón **Aplicar** no se activará si se ingresan varios rangos de IP en la **casilla Dirección de rango IP (CIDR)**.
- Expanda **Política de bloqueo de inicio de sesión**:
  1. Seleccione la casilla de verificación **Por nombre de usuario** para evitar que con un nombre de usuario específico se inicie sesión en OpenManage Enterprise.
  2. Seleccione la casilla de verificación **Por dirección IP** para evitar que con una dirección IP específica se inicie sesión en OpenManage Enterprise.
  3. En la casilla **Conteo de fallas de bloqueo**, ingrese la cantidad de intentos incorrectos después de los cuales OpenManage Enterprise debe impedir que el usuario vuelva a intentar iniciar sesión. De manera predeterminada, 3 intentos.
  4. En la casilla **Ventana de falla de bloqueo**, ingrese el tiempo durante el cual OpenManage Enterprise debe mostrar información acerca de un intento fallido.
  5. En la casilla **Tiempo de espera de bloqueo**, ingrese el tiempo durante el cual se impide al usuario realizar cualquier intento de inicio de sesión después de varios intentos incorrectos.
  6. Haga clic en **Aplicar**. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Administración de preferencias de consola

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Preferencias de la consola**, puede establecer las propiedades predeterminadas de la interfaz gráfica de usuario de OpenManage Enterprise. Por ejemplo, la hora predeterminada después de la cual la condición de un dispositivo se comprueba y actualiza automáticamente en el panel, y se usa la configuración preferida para detectar un dispositivo. Las siguientes opciones se encuentran disponibles:

1. **Ajustes de informes:** para establecer el número máximo de filas que se pueden ver en los informes de OpenManage Enterprise:
   a. Expanda la **Configuración del informe**.

b. Ingrese un número en la casilla **Límite de filas de informes**. El límite predeterminado se establece en 1.000 filas; sin embargo, las filas máximas permitidas son 2.000.000.000.
c. Haga clic en **Aplicar**. Se ejecuta una tarea y se aplica el valor.

2. **Estado del dispositivo:** para establecer la hora después de la cual el estado de los dispositivos se debe supervisar y actualizar automáticamente en el panel de OpenManage Enterprise:
   a. Expanda **Condición de los dispositivos**.
   b. Ingrese la frecuencia con que se debe registrar la condición de los dispositivos y almacenar los datos.
   c. Seleccione:
      - **Última condición conocida**: muestra la última condición registrada de los dispositivos cuando se pierde la conexión de alimentación.
      - **Desconocido**: mostrar la última condición registrada del dispositivo cuando el estado del dispositivo se mueve a "desconocido". Un dispositivo se convierte en desconocido para OpenManage Enterprise cuando se pierde la conexión con iDRAC y el dispositivo ya no se supervisa en OpenManage Enterprise.
   d. Haga clic en **Aplicar** para guardar los cambios realizados en la configuración o haga clic en **Descartar** para conservar la configuración predeterminada.
3. **Ajuste de la detección:** expanda Ajuste de la detección para establecer la nomenclatura de dispositivos que utiliza OpenManage Enterprise para identificar las iDRAC detectadas y otros dispositivos mediante los ajustes **Nombres generales de dispositivos** y **Nombres de dispositivos del servidor**.

   NOTA: Las opciones de nombres de dispositivos en Nombres generales de dispositivos y Nombres de dispositivos del servidor son independientes una de la otra y no inciden en la otra.

   a. **Nombres generales de dispositivos** se aplica a todos los dispositivos detectados que no sean de iDRAC. Seleccione uno de los siguientes modos de nombre:
      - **DNS** para utilizar el nombre DNS.
      - **Instrumentación (NetBIOS)** para utilizar el nombre de NetBIOS.

      NOTA:
      - El ajuste predeterminado de Nombres generales de dispositivos es **DNS**.
      - Si alguno de los dispositivos detectados no tiene el nombre DNS o el nombre de NetBIOS para cumplir el ajuste, entonces el dispositivo identifica aquellos dispositivos por sus direcciones IP.
      - Cuando se selecciona la opción **Instrumentación (NetBIOS)** en **Nombres generales de dispositivos**, en el caso de los dispositivos de chasis, se muestra el **nombre del chasis** como la entrada del nombre del dispositivo en la página Todos los dispositivos.

   b. **Nombres de dispositivos del servidor** solo se aplica a los iDRAC. Seleccione uno de los siguientes modos de nombres para las iDRAC detectadas:
      - **Nombre de host del iDRAC** para usar el nombre de host del iDRAC.
      - **Host del sistema** para utilizar el nombre de host del sistema.

      NOTA:
      - La preferencia de nombres predeterminados de los dispositivos iDRAC es el **Nombre de host del sistema**.
      - Si alguno de los iDRAC no tiene el nombre de host del iDRAC o el nombre de host del sistema para cumplir el ajuste, entonces el dispositivo identifica los iDRAC mediante sus direcciones IP.

   c. Para especificar los nombres de host de dispositivos que no son válidos y las direcciones MAC comunes, expanda la **Configuración avanzada**.
      i. Ingrese uno o varios nombres de host no válidos separados por comas para **Nombre de host de dispositivo no válido**. De manera predeterminada, se completa una lista de nombres de host no válidos del dispositivo.
      ii. Ingrese las direcciones MAC comunes separadas por comas en **Direcciones MAC comunes**. De manera predeterminada, se completa una lista de direcciones MAC comunes.
   d. Haga clic en **Aplicar** para guardar los cambios en la configuración o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.
4. **Detección iniciada por servidor**. Seleccione una de las siguientes políticas de aprobación de detecciones:
   - **Automático**: para permitir que la consola detecte automáticamente los servidores con la versión del firmware 4.00.00.00 de la iDRAC que se encuentren en la misma red que la consola.
   - **Manual**: para que el usuario detecte manualmente los servidores.
   - Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.
5. **Preferencias de incorporación de MX7000**: especifique uno de los siguientes comportamientos de reenvío de alertas en los chasis MX7000 cuando estos se incorporen:
   - Recibir todas las alertas
   - Recibir solo las alertas de categoría de “chasis”

6. **Ajustes de SMB:** para seleccionar una versión de Server Message Block (SMB) que se debe usar para la comunicación de red:
   - **Desactivar V1**: se desactiva SMBv1. Esta es la selección predeterminada en el dispositivo.
   - **Activar V1**: para activar SMBv1.

   NOTA: Asegúrese de habilitar SMBv1 en la **Configuración de SMB** antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte Administración de preferencias de consola en la página 163 y Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge en la página 184 para obtener más información.
7. **Ajustes del remitente de correo electrónico**: para establecer la dirección del usuario que envía un mensaje de correo electrónico:
   a. Ingrese una dirección de correo electrónico en el cuadro **ID de correo electrónico del remitente**.
   b. Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.
8. **Formato de reenvío de trap**: para establecer el formato de reenvío de trap:
   a. Seleccione una de las siguientes opciones
      - **Formato original (válido solo para trap de SNMP)**: para conservar los datos de trap tal como están.
      - **Normalizado (válido para todos los eventos)**: se utiliza para normalizar los datos de captura. Cuando el formato de reenvío de capturas se configura en "Normalizado", el agente receptor, como el registro del sistema, recibe una etiqueta que contiene la dirección IP del dispositivo desde la cual se reenvió la alerta.
   b. Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.
9. **Configuración de recopilación de métricas**: para establecer la frecuencia de mantenimiento y depuración de los datos de la extensión de PowerManager, realice lo siguiente:
   a. En el cuadro **Intervalo de depuración de datos**, ingrese la frecuencia con la que desea eliminar los datos de PowerManager. Puede ingresar valores comprendidos entre 30 y 365 días.
   b. Haga clic en **Aplicar** para guardar los cambios o en **Descartar** para restablecer la configuración a los atributos predeterminados.

Personalizar la visualización de alertas

1. Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación>Alertas** y expanda **Configuración de visualización de alertas**.
2. Seleccione una de las siguientes opciones:
   a. **Todas**: para habilitar la visualización de alertas confirmadas y no confirmadas.
   b. **No confirmadas**: para habilitar la visualización solo de alertas no confirmadas.

      NOTA: De manera predeterminada, la **Configuración de la visualización de alertas** está definida en **No confirmadas**.

   c. **Confirmadas**: para habilitar la visualización solo de alertas confirmadas.
3. Haga clic en **Aplicar**.

   Los cambios en la configuración de la visualización de alertas tendrán efecto en las siguientes páginas de OpenManage Enterprise:
   - En la esquina superior derecha de todas las páginas de OpenManage Enterprise. Consulte Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise en la página 35.
   - En la página Panel. Consulte Monitoreo de dispositivos mediante el panel de OpenManage Enterprise en la página 37.
   - En la página Dispositivos. Consulte Gráfico de anillo en la página 38.
   - En la tabla **Registro de alertas** de la página Alertas. Consulte Visualización del registro de alertas en la página 117.

Configurar alertas de SMTP, SNMP y registro del sistema

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Alertas**, puede configurar la dirección de correo electrónico (SMTP) que recibe las alertas del sistema, los destinos de reenvío de alertas SNMP y las propiedades de reenvío de Syslog. Para administrar estas configuraciones, debe contar con credenciales de nivel de administrador de OpenManage Enterprise.

Para configurar y autenticar el servidor SMTP que administra la comunicación por correo electrónico entre los usuarios y OpenManage Enterprise, haga lo siguiente:

1. Expanda **Configuración de correo electrónico**.
2. Ingrese la dirección de red del servidor SMTP que envía mensajes de correo electrónico.

3. Para autenticar el servidor SMTP, seleccione la casilla de verificación **Activar autenticación** e ingrese el nombre de usuario y la contraseña.
4. De manera predeterminada, el número de puerto SMTP al que se debe acceder es 25. Edite según sea necesario.
5. Seleccione la casilla de verificación **Utilizar SSL** para proteger la transacción SMTP.
6. Para probar si el servidor SMTP funciona correctamente, haga clic en la casilla de verificación **Enviar correo electrónico de prueba** e ingrese un **destinatario de correo electrónico**.
7. Haga clic en **Aplicar**.
8. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para configurar los ajustes de reenvío de alertas SNMP, haga lo siguiente:

1. Expanda **Configuración de reenvío de alertas SNMP**.
2. Seleccione la casilla de verificación **HABILITADA** para habilitar las capturas SNMP respectivas para enviar alertas en caso de sucesos predefinidos.
3. En la casilla **DIRECCIÓN DE DESTINO**, ingrese la dirección IP del dispositivo de destino que debe recibir la alerta.

   NOTA: No se permite ingresar la IP de la consola para evitar la duplicación de alertas.
4. En el menú **VERSIÓN DE SNMP**, seleccione el tipo de versión de SNMP como SNMPv1, SNMPv2 o SNMPv3, y complete los campos a continuación:
   a. En el cuadro CADENA DE COMUNIDAD, ingrese la cadena de comunidad SNMP del dispositivo que debe recibir la alerta.
   b. Edite el NÚMERO DE PUERTO, si es necesario. El número de puerto predeterminado para las capturas SNMP es 162. Consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
   c. Si se selecciona SNMPv3, proporcione los siguientes detalles adicionales:
      i. NOMBRE DE USUARIO: proporcione un nombre de usuario.
      ii. TIPO DE AUTENTICACIÓN: en la lista desplegable, seleccione SHA, MD_5 o Ninguno.
      iii. FRASE DE CONTRASEÑA DE AUTENTICACIÓN: proporcione una frase de contraseña de autenticación con un mínimo de ocho caracteres.
      iv. TIPO DE PRIVACIDAD: en la lista desplegable, seleccione DES, AES_128 o Ninguno.
      v. FRASE DE CONTRASEÑA DE PRIVACIDAD: proporcione una frase de contraseña de privacidad con un mínimo de ocho caracteres.
5. Para probar un mensaje SNMP, haga clic en el botón **Enviar** de la captura correspondiente.
6. Haga clic en **Aplicar**. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para actualizar la configuración de reenvío de registro del sistema, haga lo siguiente:

1. Expanda **Configuración de reenvío de Syslog**.
2. Seleccione la casilla de verificación para habilitar la característica de Syslog en el servidor correspondiente en la columna **SERVIDOR**.
3. En la casilla **DIRECCIÓN/NOMBRE DE HOST DE DESTINO**, ingrese la dirección IP del dispositivo que recibe los mensajes de Syslog.
4. Se accede al número de puerto predeterminado cuando UDP equivale a 514. Ingrese o seleccione en la casilla, si fuera necesario editar. Consulte Protocolos y puertos admitidos en OpenManage Enterprise en la página 32.
5. Haga clic en **Aplicar**.
6. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Administración de alertas entrantes

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16.

Si hace clic en **OpenManage Enterprise** > **Ajustes de la aplicación** > **Alertas entrantes**, puede establecer las propiedades de TrapForward y definir el usuario que recibe las alertas SNMPv3 entrantes.

- Para establecer las credenciales de SNMP para las alertas entrantes:

1. Seleccione la casilla de verificación **Habilitar SNMPV3**.
2. Haga clic en **Credenciales**.
3. En el cuadro de diálogo **Credenciales de SNMP**:
   a. En la casilla **Nombre de usuario**, ingrese el ID de inicio de sesión del usuario que administra la configuración de OpenManage Enterprise.
   b. En el menú desplegable **Tipo de autenticación**, seleccione el algoritmo **SHA** o **MD_5** como el tipo de autenticación.
   c. En la casilla **Frase de contraseña de autenticación**, ingrese la frase de contraseña que está relacionada con SHA o MD_5 según su selección.
   d. En el menú desplegable **Tipo de privacidad**, seleccione DES o AES_128 como su cifrado estándar.

e. En la casilla **Frase de contraseña de privacidad**, ingrese la frase de contraseña según su tipo de privacidad.
f. Haga clic en **Guardar**.

4. En la casilla **Comunidad**, ingrese la cadena de comunidad que debe recibir las capturas SNMP.
5. De manera predeterminada, el número de puerto SNMP para las capturas entrantes es 162. Edite para cambiar el número de puerto.
6. Haga clic en **Aplicar**.
   Se guardan las credenciales SNMP y la configuración.
7. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

   NOTA: Si los ajustes de alertas de SNMPv3 se configuran antes de actualizar el dispositivo, es posible que deba volver a configurar los ajustes mediante el nombre de usuario, una frase de contraseña de autenticación y una frase de contraseña de privacidad para seguir recibiendo las alertas. Si el problema persiste, reinicie los servicios mediante la interfaz de usuario de texto (TUI).

8. Haga clic en **Aplicar** para guardar los cambios o en **Descartar** para cancelarlos.

Configuración de credenciales de SNMP

1. Haga clic en **Credenciales**.
2. En el cuadro de diálogo **Credenciales de SNMP**:
   a. En la casilla **Nombre de usuario**, ingrese el ID de inicio de sesión del usuario que administra la configuración de OpenManage Enterprise.
   b. En el menú desplegable **Tipo de autenticación**, seleccione el algoritmo **SHA** o **MD_5** como el tipo de autenticación.
   c. En la casilla **Frase de contraseña de autenticación**, ingrese la frase de contraseña que está relacionada con SHA o MD_5 según su selección.
   d. En el menú desplegable **Tipo de privacidad**, seleccione DES o AES_128 como su cifrado estándar.
   e. En la casilla **Frase de contraseña de privacidad**, ingrese la frase de contraseña según su tipo de privacidad.
3. Haga clic en **Guardar**.

Administración de la configuración de garantía

La **Configuración de la garantía** determina la visualización de las estadísticas de la garantía por parte de OpenManage Enterprise en el widget de Alerta de la página de inicio, el cuadro de mandos en todas las páginas, la página Garantía y los informes.

Para cambiar la configuración de la garantía, realice los siguientes pasos:

1. Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Garantía**
2. Haga clic en **Configuración de la garantía** para activar el cuadro de diálogo.
3. En el cuadro **Mostrar advertencia si las garantías expiran en los próximos**, ingrese el número de días. Puede ingresar un valor entre 0 y 1000 (ambos incluidos). El valor predeterminado es de 90 días. Las garantías que caducan según esta configuración se representan como ⚠ en el informe y el widget.
4. Desde las opciones **Ocultar las garantías caducadas**, puede seleccionar una de las siguientes opciones:
   a. **Todas**: para ocultar la visualización de todas las garantías "iniciales" y "extendidas" que caducaron.
   b. **Solo iniciales**: para ocultar solo las garantías "iniciales" que caducaron.
   c. **Ninguna**: para mostrar todas las garantías que caducaron.
5. Haga clic en **Aplicar** o **Descartar** para guardar la configuración de la garantía o para descartar los cambios y conservar la configuración anterior.

Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles

Para ir a la página Consola y plugins, haga clic en **Configuración de la aplicación** > **Consola y plugins**. En la página Consola y plugins, puede hacer lo siguiente:

1. Ver la versión actual de su OpenManage Enterprise, comprobar si hay actualizaciones disponibles y, luego, actualizar a una versión más reciente. Puede hacer clic en el botón **Actualizar configuración** para realizar lo siguiente:

a. Comprobar si hay actualizaciones de forma automática o manual.
b. Elegir los modos En línea o Sin conexión para actualizar el dispositivo.

Para obtener más información, consulte Actualizar los ajustes en OpenManage Enterprise en la página 168

2. Descargue e instale más plugins (complementos), como el plugin Power Manager, para mejorar la funcionalidad del dispositivo. Para obtener más información acerca de la instalación de plugins, consulte plugin

   NOTA: Se requiere la licencia de OpenManage Enterprise Advanced para que los plugins funcionen en su totalidad después de la instalación. Para obtener información más detallada sobre los plugins, consulte la documentación correspondiente disponible en el sitio de soporte de Dell.

   NOTA: Si instala un plug-in en OpenManage Enterprise, se reiniciarán los servicios del dispositivo.

3. Con los plugins ya instalados, puede hacer lo siguiente:

- Haga clic en el menú desplegable **Más acciones** para obtener más información acerca del plugin, o bien para deshabilitar, desinstalar, habilitar o cambiar la configuración del plugin. Para obtener más información, consulte plugin, plugin, plugin
- Puede hacer clic en **Actualización disponible** siempre y cuando haya disponible nuevas versiones de los plugins.

Información relacionada

Actualización de Dell.com en la página 170
Actualización de un recurso compartido de red interna en la página 170

Actualizar los ajustes en OpenManage Enterprise

Cuando hace clic en **Ajustes de configuración** en la página Consola y extensiones (**Ajustes de la aplicación** > **Consola y extensiones**), se pueden seleccionar los siguientes ajustes de actualización:

1. **Cómo buscar actualizaciones**: seleccione entre los siguientes métodos:
   a. **Automático**: el dispositivo comprueba la disponibilidad de las actualizaciones automáticamente todos los lunes desde la fuente especificada en **Dónde buscar actualizaciones**.
   b. **Manual**: cuando se configura en Manual, el usuario tiene que comprobar manualmente la disponibilidad de la actualización de la fuente especificada en **Dónde buscar actualizaciones**.
2. **Dónde buscar actualizaciones**: se puede especificar la ubicación desde donde el dispositivo busca actualizaciones. Las siguientes opciones se encuentran disponibles:
   a. **Dell.com** (en línea): cuando se selecciona esta opción, el dispositivo comprueba la disponibilidad de la actualización directamente desde https://downloads.dell.com/openmanage_enterprise.
   b. **Recurso compartido de red** (offline): especifique una ruta de acceso NFS, HTTP o HTTPS que contenga el paquete de actualización. Haga clic en **Probar ahora** para validar la conexión al recurso compartido de red especificado.

   NOTA: En el caso de las actualizaciones offline (recurso compartido de red), el administrador debe crear estructuras de carpetas adecuadas antes de descargar el paquete de actualización dependiendo de si se necesita una actualización mínima o completa. Para obtener más información sobre cómo actualizar OpenManage Enterprise a la versión más reciente y de las estructuras de carpetas permitidas para actualizaciones, consulte la documentación técnica Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) en el sitio de soporte.

3. Seleccione la casilla de verificación **Iniciar automáticamente la actualización de la consola cuando se completen las descargas** para iniciar la instalación de la actualización de la consola inmediatamente después de descargar el paquete de actualización. Por lo demás, la actualización se puede iniciar manualmente.

   NOTA: Según los ajustes de la actualización, el dispositivo comprueba la disponibilidad de una actualización y, si hay una nueva versión disponible, se muestra un anuncio con la información de la nueva versión de actualización. En el anuncio, el administrador puede optar por descartar la notificación, solicitar un recordatorio para más tarde o hacer clic en **Ver ahora** para conocer los detalles, como la versión y el tamaño de la actualización disponible en la página **Ajustes de la aplicación** > **Consola y extensiones**. En la sección OpenManage Enterprise de la página de la Consola y extensiones, se muestran todas las nuevas funciones y mejoras de la actualización disponible. Haga clic en **Actualizar** para iniciar la actualización.

Actualizar OpenManage Enterprise

Según los ajustes de la actualización (**Ajustes de la aplicación** > **Consola y extensiones** > **Ajustes de la actualización)**, el OpenManage Enterprise existente se puede actualizar de forma automática o manual desde el sitio Dell.com directamente o desde un paquete de actualización ya descargado en el recurso compartido de red.

Cuando se identifica una versión nueva y actualizable de OpenManage Enterprise, se muestran detalles adicionales, como la versión, el tamaño y las nuevas funciones de la actualización, en la página Consola y extensiones, y hay un botón de **actualización** activo disponible. Además, se muestra un anuncio con detalles de la nueva versión. Todos los usuarios pueden ver el anuncio, sin embargo, solo los usuarios con privilegio de administrador pueden seleccionar la opción para recordar más tarde o descartar el mensaje.

NOTA:

- Solo las versiones 3.4 y posteriores de OpenManage Enterprise se pueden actualizar directamente a la versión 3.6 mediante el método **Automático** > **En línea**.
- Las versiones de OpenManage Enterprise anteriores a la versión 3.4, por ejemplo, la versión 3.3x y la versión 3.2, primero se deben actualizar a la versión 3.4 antes de considerar la actualización a 3.6.
- No se admite una actualización directa de la versión OpenManage Enterprise Tech Release. La versión Tech Release se debe actualizar primero a la versión 3.0 o 3.1 de OpenManage Enterprise.
- Después de actualizar a la versión 3.6, los administradores de dispositivos existentes tendrán todos los dispositivos que se encuentran dentro de su alcance de forma predeterminada. Sin embargo, si es necesario, el administrador puede editar el alcance de los administradores de dispositivos mediante la función SBAC. Para obtener más información, consulte Control de acceso basado en funciones y en el alcance en OpenManage Enterprise en la página 16 y Administración de usuarios de OpenManage Enterprise en la página 147.

Antes de actualizar a la versión más reciente, el administrador debería:

- Tome una captura de la consola en la máquina virtual como copia de seguridad en caso de que ocurriera algo inesperado. Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario.
- Asigne por lo menos una hora para el proceso de actualización. Asigne tiempo adicional si se debe descargar la actualización mediante una conexión de red más lenta.
- Asegúrese de que no se ejecuten tareas de configuración, implementación o extensión (plugin) de dispositivos ni que se programen sus respectivas ejecuciones durante el tiempo de inactividad planificado. Todas las políticas o tareas activas o programadas se cierran sin advertencia durante la actualización.
- Notifique a los demás usuarios de la consola sobre la próxima actualización programada.
- Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente.

Para actualizaciones de OpenManage Enterprise versión 3.5, el resultado del proceso de actualización se indica mediante un anuncio en las páginas de la consola. De manera predeterminada, el anuncio se muestra durante 24 horas después de la actualización; sin embargo, puede borrarlo si hace clic en “Descartar” en el extremo derecho del anuncio. Cuando la actualización de OpenManage Enterprise versión 3.5 se realiza correctamente, el anuncio se muestra en verde y el mensaje “actualización correcta” indica el nuevo número de versión del dispositivo. Sin embargo, si la actualización falla, el dispositivo se restaura automáticamente a su versión anterior y el anuncio se muestra en naranja y con un mensaje de “error”. Puede hacer clic en “Ver detalles” en el anuncio para ver el historial de ejecución del trabajo de actualización en la página Detalles del trabajo.

NOTA:

- Cuando actualice OpenManage Enterprise y cuente con más de 8,000 dispositivos detectados, la tarea de actualización se completará dentro de dos o tres horas. Durante este período, es posible que los servicios no respondan. Se recomienda reiniciar el dispositivo de forma ordenada. Después de reiniciarlo, la funcionalidad normal del dispositivo se restaura.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de descubrimiento se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.
- Cuando hace clic en **Actualizar**, se inicia un trabajo de Descarga del paquete de actualización. Este trabajo se completa por su cuenta después de que se descarguen todos los archivos de actualización y el usuario no puede finalizarlo.

1. Para actualizar en línea desde Dell.com, consulte Actualización de Dell.com en la página 170.
2. Para realizar la actualización offline desde un paquete de actualización ya descargado en el recurso compartido de red NFS o HTTPS, consulte Actualización de un recurso compartido de red interna en la página 170.

NOTA: Según si se necesita una actualización mínima o completa, el administrador deber crear las estructuras de carpetas adecuadas antes de descargar el paquete de actualización. Para obtener más información acerca de las estructuras de carpetas permitidas y la actualización de OpenManage Enterprise a la versión más reciente, consulte la documentación técnica *Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise* en el sitio de soporte.

Actualización de Dell.com

El OpenManage Enterprise existente se puede actualizar en línea, ya sea de forma automática o manual, desde Dell.com (https://downloads.dell.com/openmanage_enterprise).

Requisitos previos para la actualización en línea:

- Los ajustes de la actualización **Dónde buscar actualizaciones** se debe especificar como Dell.com. Para obtener más información, consulte Actualizar los ajustes en OpenManage Enterprise en la página 168.
- Debe asegurarse de que el dispositivo OpenManage Enterprise pueda acceder a Dell.com y a la actualización prevista.
- Antes de comenzar la actualización, asegúrese de tomar una captura de la consola en la máquina virtual como respaldo en caso de que ocurra algo inesperado. Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario.

Cuando se identifica una versión nueva y actualizable de OpenManage Enterprise, se muestran detalles adicionales, como la versión, el tamaño y las nuevas funciones de la actualización, en la página Consola y extensiones, y hay un botón de **actualización** activo disponible. Además, se muestra un anuncio con detalles de la nueva versión. Todos los usuarios pueden ver el anuncio, sin embargo, solo los usuarios con privilegio de administrador pueden seleccionar la opción para recordar más tarde o descartar el mensaje.

1. Haga clic en **Actualizar** y realice una actualización.

   NOTA:
   - Cuando hace clic en **Actualizar**, se inicia un trabajo de Descarga del paquete de actualización. Este trabajo se completa por sí mismo después de que se descarguen todos los archivos de actualización y no se puede finalizar.
   - Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente

2. Inicie sesión después de la actualización y confirme que el producto funcione según lo esperado. Compruebe el registro de auditoría de todas las advertencias o los errores relacionados con la actualización. Si se producen errores, exporte el registro de auditoría y guárdelo para solicitar asistencia técnica.

Una vez que se actualiza el dispositivo:

- Borre la caché del explorador. Si no borra la memoria caché del navegador, es posible que ocurran errores en las tareas nuevas después de la actualización.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de descubrimiento se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.

Tareas relacionadas

Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167

Actualización de un recurso compartido de red interna

Debe configurar un recurso compartido de red local y descargar manualmente el paquete de actualización cuando no se conecta automáticamente a Dell.com. Se crea un registro de auditoría después de cada intento de buscar una actualización manualmente.

NOTA:
- Las versiones de OpenManage Enterprise anteriores a la 3.4, por ejemplo, la versión 3.3x y la versión 3.2, primero se deben actualizar a la versión 3.4 antes de considerar la actualización a 3.6 a través de un Recurso compartido de archivos de red (NFS) compartido.
- No se admite una actualización directa de la versión OpenManage Enterprise Tech Release. La versión Tech Release se debe actualizar primero a la versión 3.0 o 3.1 de OpenManage Enterprise.
- En el caso de las actualizaciones offline (recurso compartido de red), el administrador debe crear estructuras de carpetas adecuadas antes de descargar el paquete de actualización dependiendo de si se necesita una actualización mínima o

completa. Para obtener más información sobre cómo actualizar OpenManage Enterprise a la versión más reciente y de las estructuras de carpetas permitidas para actualizaciones, consulte la documentación técnica Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf) en el sitio de soporte.

- Cuando se actualizan recursos compartidos locales en una actualización manual de las versiones sin extensiones o complementos instalados (como 3.1 y 3.2), el registro de auditoría muestra entradas de advertencia, como "no se puede recuperar el archivo de origen del tipo catálogo de extensión porque el archivo no existe" y "el estado de descarga del catálogo de extensión contiene errores". Estos mensajes de error no tienen ningún impacto funcional en el proceso de actualización y se pueden omitir.

Antes de comenzar la actualización:

- asegúrese de tomar una instantánea de la consola en la máquina virtual como respaldo en caso de que ocurra algo inesperado. (Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario).
- Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.
- Debe asegurarse de que los certificados de seguridad estén firmados por una autoridad de certificación de terceros de confianza cuando utilice el método de actualización HTTPS.

Para actualizar OpenManage Enterprise, realice las siguientes acciones:

1. Descargue los archivos correspondientes en https://downloads.dell.com, guárdelos en un recurso compartido de red y conserve la misma estructura de carpetas a la que se puede acceder a través de la consola.
2. Seleccione **Manual** y **Offline**.
3. Ingrese la información de la ruta local en la que se guardan los archivos descargados y, a continuación, haga clic en **Comprobar ahora**. Rutas de ejemplo: *nfs://<Dirección IP>/<Nombre_carpeta>*, *http://<Dirección IP>/<Nombre_carpeta>*, *https://<Dirección IP>/<Nombre_carpeta>*.
   Se muestra la versión de actualización disponible con una breve descripción de las nuevas funciones.
4. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se establece la conexión con el catálogo, aparecerá el mensaje *Conexión correcta*. Si no se establece la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparecerá el mensaje *Error de conexión a la ruta*. Este paso es opcional.
5. Haga clic en **Actualizar** y realice una actualización (aplicable para futuras actualizaciones).

   NOTA:
   - Cuando hace clic en **Actualizar**, se inicia un trabajo de Descarga del paquete de actualización. Este trabajo finaliza por su cuenta después de que se descargan todos los archivos de actualización y el usuario no puede finalizarlo
   - Si durante la descarga de la actualización ocurre un problema de conexión a través de proxy, desmarque la configuración de proxy y, luego, realice la descarga.

Inicie sesión después de la actualización y confirme que el producto funcione según lo esperado. Compruebe el registro de auditoría de todas las advertencias o los errores relacionados con la actualización. Si se producen errores, exporte el registro de auditoría y guárdelo para solicitar asistencia técnica.

Una vez que se actualiza el dispositivo:

- Borre la caché del explorador. Si no borra la memoria caché del navegador, es posible que ocurran errores en las tareas nuevas después de la actualización.
- Si realiza la actualización desde OpenManage Enterprise versión 3.1, se recomienda volver a configurar o importar los grupos de Active Directory para mejorar el rendimiento.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de descubrimiento se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.

Tareas relacionadas

Comprobar y actualizar la versión de OpenManage Enterprise y los plugins disponibles en la página 167

Instalar un plugin

Puede instalar los plug-ins Power Manager, SupportAssist-Enterprise y Update Manager en función de sus requisitos para mejorar la funcionalidad de OpenManage Enterprise.

- Para instalar los plug-ins de OpenManage Enterprise desde Dell.com, asegúrese de que el dispositivo OpenManage Enterprise pueda acceder a downloads.dell.com.
- Para instalar los plug-ins de OpenManage Enterprise desde un recurso compartido de red local, debe descargar manualmente el paquete en el recurso compartido de red y actualizar la ubicación en la página Ajustes de actualización de OpenManage Enterprise.

Para obtener más información sobre la configuración de Ajustes de actualización, consulte Actualizar los ajustes en OpenManage Enterprise en la página 168.

NOTA: Si instala un plug-in en OpenManage Enterprise, se reiniciarán los servicios del dispositivo.

Para instalar un plug-in, complete los siguientes pasos:

1. En OpenManage Enterprise, haga clic en **Ajustes de la aplicación** > **Consola y plug-ins**
   Se muestra la página **Consola y plug-ins**.
2. En la sección **Plug-ins**, haga clic en la opción **Instalar** para el plug-in que desea instalar.
   Se muestra el asistente para **Instalar plug-in**.
3. En la lista **Versiones disponibles**, seleccione la versión que desea instalar.
4. Revise la sección **Requisitos previos** y asegúrese de que cumple con la lista de requisitos previos que se menciona ahí; luego haga clic en **Descargar plug-in**.

   NOTA: Las listas de requisitos cambian a medida que selecciona la versión del plugin que desea instalar.

   La operación de instalación valida los requisitos previos para instalar el plug-in. Si no se cumplen los requisitos previos de instalación, se muestra el mensaje de error correspondiente.

   Una vez que se descarga correctamente el plug-in, el estado que aparece en la parte superior del plug-in cambia de **Disponible** a **Descargado**.
5. A fin de instalar el plug-in de OpenManage Enterprise, en el asistente para **Instalar plug-in**, haga clic en **Instalar plug-in**.
6. Se muestra un formulario de consentimiento para informarle sobre el end user license agreement (EULA). Haga clic en **Aceptar** para continuar con la instalación del plug-in.
   En el cuadro de diálogo **Confirmación**, se muestran detalles sobre la cantidad de usuarios que iniciaron sesión en OpenManage Enterprise, las tareas en curso y los trabajos programados.
7. Para confirmar la instalación, seleccione **Acepto que he capturado una instantánea del dispositivo OpenManage Enterprise antes de realizar la acción de plug-in** y, luego, haga clic en **Confirmar instalación**.
   Aparece el estado de la operación de instalación. Una vez que se haya instalado correctamente el plug-in, el estado que aparece en la parte superior del plug-in cambia de **Disponible** o **Descargado** a **Instalado**.

Deshabilitar un plugin

Desactiva toda la funcionalidad del plugin en OpenManage Enterprise.

NOTA: La deshabilitación de un plugin en OpenManage Enterprise reinicia los servicios del dispositivo.

1. Inicie OpenManage Enterprise y haga clic en **Ajustes de la aplicación** > **Consola y plug-ins**.
   Se muestra la pestaña **Consola y plugins**.
2. En la sección **Plug-ins**, haga clic en la opción **Inhabilitar** para el plug-in que desea inhabilitar.
   Se muestra el asistente para **Inhabilitar plug-in**.
3. Para inhabilitar el plug-in, haga clic en **Inhabilitar plug-in**.
   En el cuadro de diálogo **Confirmación**, se muestran detalles sobre la cantidad de usuarios que iniciaron sesión en OpenManage Enterprise, las tareas en curso y los trabajos programados.
4. Para confirmar, seleccione la opción **Acepto que he capturado una instantánea del dispositivo OpenManage Enterprise antes de realizar una acción de plug-in**. A continuación, haga clic en **Confirmar inhabilitación**.

NOTA: Después de deshabilitar el plugin, no podrá ver ninguna información o página relacionada con el plugin en OpenManage Enterprise.

Desinstalar un plugin

Desinstala y elimina todos los datos que recolecta el plugin.

1. Inicie OpenManage Enterprise y haga clic en **Ajustes de la aplicación** > **Consola y plug-ins**.
   Se muestra la pestaña **Consola y plugins**.

2. En la sección **Plug-ins**, haga clic en la opción **Desinstalar** para el plug-in que desea desinstalar.
   Se muestra el asistente para **Desinstalar plug-in**.
3. Para desinstalar el plug-in desde OpenManage Enterprise, haga clic en **Desinstalar plug-in**.
   En el cuadro de diálogo **Confirmación**, se muestran detalles sobre la cantidad de usuarios que iniciaron sesión en OpenManage Enterprise, las tareas en curso y los trabajos programados.
4. Para confirmar la desinstalación, seleccione la opción **Acepto que he capturado una instantánea del dispositivo OpenManage Enterprise antes de realizar una acción de plug-in**. A continuación, haga clic en **Confirmar desinstalación**.

Se desinstalarán todas las funcionalidades y los datos asociados con el plug-in.

Habilitar plugin

Todas las páginas del plug-in se muestran en OpenManage Enterprise y la funcionalidad del plug-in está habilitada en OpenManage Enterprise.

NOTA: La habilitación de un plugin en OpenManage Enterprise reinicia los servicios del dispositivo.

1. Inicie OpenManage Enterprise y haga clic en **Ajustes de la aplicación** > **Consola y plug-ins**.
   Se muestra la pestaña **Consola y plugins**.
2. En la sección **Plug-ins**, haga clic en la opción **Habilitar** para el plug-in que desea habilitar.
   Se muestra el asistente **Habilitar plug-in**.
3. Para habilitar el plug-in, haga clic en **Habilitar plug-in**.
   En el cuadro de diálogo **Confirmación**, se muestran detalles sobre la cantidad de usuarios que iniciaron sesión en OpenManage Enterprise, las tareas en curso y los trabajos programados.
4. Para confirmar, seleccione la opción **Acepto que he capturado una instantánea del dispositivo OpenManage Enterprise antes de realizar una acción de plug-in**. A continuación, haga clic en **Confirmar habilitación**.

Actualizar un plug-in

Según los ajustes de actualización, el dispositivo comprueba la disponibilidad de una actualización de los plug-ins instalados. Si hay una nueva versión disponible, se muestra un anuncio con información de la nueva versión de actualización. En el anuncio, el administrador puede optar por descartar la notificación, solicitar un recordatorio para más tarde o hacer clic en **Ver ahora** para conocer los detalles, como la versión y el tamaño de la actualización disponible en la página **Ajustes de la aplicación** > **Consola y plug-ins**. En la sección Plug-in de la página Consola y plug-ins, se muestran todas las nuevas funciones y mejoras de la actualización de plug-ins disponible.

Antes de actualizar un plug-in, asegúrese de que los ajustes de actualización estén configurados como se mencionó en Actualizar los ajustes en OpenManage Enterprise en la página 168 .

Para actualizar un plug-in, haga lo siguiente:

1. En la sección plug-in, haga clic en **Actualización disponible** para el plug-in que desea actualizar.
   Se muestra la página **Actualizar plug-in**.
2. Seleccione la versión del plug-in y, a continuación, haga clic en **Descargar plug-in**.
   Se descarga el plug-in y el estado de la descarga se muestra en una banda de color verde.
3. Para actualizar el plug-in, haga clic en **Actualizar plug-in**.
   En la ventana **Confirmación**, seleccione la opción **Acepto que he capturado una instantánea del dispositivo OpenManage Enterprise antes de realizar una acción de plug-in** y, a continuación, haga clic en **Actualizar**.

Una vez finalizada la operación de actualización, la versión se mostrará en la sección Plug-in.

Ejecutar comandos y scripts remotos

Cuando recibe una SNMP trap, puede ejecutar un script en OpenManage Enterprise. Esto establece una política que abre un vale en el sistema de generación de vales de terceros para la administración de alertas. Puede crear y almacenar solo hasta **cuatro** comandos remotos.

NOTA: El uso de los siguientes caracteres especiales como parámetros de la CLI de IPMI y RACADM no es soportado: **[**, **;**, **|**, **$**,**>**,**<**, **&**, **'**, **]**, **.**, * y **'**.

1. Haga clic en **Configuración de la aplicación** > **Ejecución del script**.
2. En la sección **Configuración de comandos remotos**, haga lo siguiente:

a. Para agregar un comando remoto, haga clic en **Crear**.
b. En la casilla **Nombre del comando**, escriba el nombre del comando.
c. Seleccione uno de los siguientes tipos de comando:
   i. Script
   ii. RACADM
   iii. Herramienta IPMI
d. Si selecciona **Script**, haga lo siguiente:
   i. En la casilla **Dirección IP**, ingrese la dirección IP.
   ii. Seleccione el método de autenticación: **contraseña** o **clave SSH**.
   iii. Especifique el **Nombre de usuario** y la **Contraseña** o la **clave SSH**.
   iv. En la casilla **Comando**, escriba los comandos.
      - Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
      - La sustitución de token en secuencias de comandos es posible. Consulte Sustitución del token en secuencias de comandos remotas y política de alerta en la página 181
   v. Haga clic en **Finalizar**.
e. Si selecciona **RACADM**, haga lo siguiente:
   i. En la casilla **Nombre del comando**, escriba el nombre del comando.
   ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
   iii. Haga clic en **Finalizar**.
f. Si selecciona **Herramienta IPMI**, haga lo siguiente:
   i. En la casilla **Nombre del comando**, escriba el nombre del comando.
   ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
   iii. Haga clic en **Finalizar**.

3. Para editar la configuración de los comandos remotos, seleccione el comando y haga clic en **Editar**.
4. Para eliminar la configuración de los comandos remotos, seleccione el comando y haga clic en **Eliminar**.

Configuración de OpenManage Mobile

OpenManage Mobile (OMM) es una aplicación de administración de sistemas que permite realizar de forma segura un subconjunto de tareas de reparación y supervisión de los centros de datos en una o varias consolas de OpenManage Enterprise o integrated Dell Remote Access Controllers (iDRAC) mediante un dispositivo Android o iOS. Mediante OMM puede:

- Recibir notificaciones de alertas desde OpenManage Enterprise.
- Ver información del grupo, el dispositivo, alertas y registros.
- Encender, apagar o reiniciar un servidor.

De manera predeterminada, las notificaciones de inserción están activadas para todas las alertas y las alertas críticas. Este capítulo proporciona información sobre los ajustes de OMM que puede configurar a través de OpenManage Enterprise. También proporciona información necesaria para solucionar los problemas de OMM.

NOTA: Para obtener información sobre la instalación y el uso de OMM, consulte la *Guía del usuario de OpenManage Mobile* en Dell.com/OpenManageManuals.

Tareas relacionadas

Activación o desactivación de notificaciones de alerta de OpenManage Mobile en la página 175
Activación o desactivación de suscriptores de OpenManage Mobile en la página 175
Eliminación de un suscriptor de OpenManage Mobile en la página 175
Visualización del estado del servicio de notificación de alertas en la página 176
Solución de problemas de OpenManage Mobile en la página 177

Información relacionada

Activación o desactivación de notificaciones de alerta de OpenManage Mobile en la página 175
Activación o desactivación de suscriptores de OpenManage Mobile en la página 175
Solución de problemas de OpenManage Mobile en la página 177

Activación o desactivación de notificaciones de alerta de OpenManage Mobile

De manera predeterminada, OpenManage Enterprise está configurado para enviar notificaciones de alerta a la aplicación OpenManage Mobile. Sin embargo, las notificaciones de alerta se envían desde OpenManage Enterprise solo cuando un usuario de OpenManage Mobile agrega OpenManage Enterprise a la aplicación de OpenManage Mobile.

NOTA: Se requieren privilegios de administrador para activar o desactivar las notificaciones de alerta en OpenManage Mobile.

NOTA: Para que OpenManage Enterprise envíe notificaciones de alerta a OpenManage Mobile, asegúrese de que el servidor de OpenManage Enterprise tenga acceso a Internet (HTTPS) de salida.

Para activar o desactivar las notificaciones de alerta de OpenManage Enterprise a OpenManage Mobile, realice lo siguiente:

1. Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Móvil**.
2. Marque la casilla **Activar envío de notificaciones push**.
3. Haga clic en **Aplicar**.

Tareas relacionadas

Configuración de OpenManage Mobile en la página 174

Información relacionada

Configuración de OpenManage Mobile en la página 174
Eliminación de un suscriptor de OpenManage Mobile en la página 175

Activación o desactivación de suscriptores de OpenManage Mobile

Las casillas de verificación de la columna **Activado** en la lista de **Suscriptores móviles** le permiten activar o desactivar la transmisión de notificaciones de alerta a los suscriptores de OpenManage Mobile.

NOTA:

- Se requieren los privilegios del administrador para activar o desactivar suscriptores de OpenManage Mobile.
- OpenManage Enterprise puede desactivar automáticamente a los suscriptores de OpenManage Mobile si el servicio de notificación push de su proveedor de servicios móviles indica que el dispositivo está permanentemente inaccesible.
- Incluso si un suscriptor de OpenManage está activado en la lista de **Suscriptores móviles**, pueden desactivar la recepción de la notificación de alertas en sus valores de la aplicación OpenManage Mobile.

Para activar o desactivar las notificaciones de alerta para los suscriptores de OpenManage Mobile:

1. Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Móvil**.
2. Para activar, seleccione la casilla de verificación correspondiente y haga clic en **Activar**. Para desactivar, seleccione la casilla de verificación y, a continuación, haga clic en **Desactivar**.

   Puede seleccionar más de un suscriptor por vez.

Tareas relacionadas

Configuración de OpenManage Mobile en la página 174

Información relacionada

Configuración de OpenManage Mobile en la página 174
Eliminación de un suscriptor de OpenManage Mobile en la página 175

Eliminación de un suscriptor de OpenManage Mobile

Si se elimina un suscriptor de OpenManage Mobile, se elimina al usuario de la lista de suscriptores, lo que impide que este reciba las notificaciones de alerta de OpenManage Enterprise. Sin embargo, el usuario de OpenManage Mobile puede volver a suscribirse más tarde a las notificaciones de alerta desde la aplicación OpenManage.

NOTA: Se requieren derechos de administrador para eliminar a un suscriptor de OpenManage Mobile.

Para eliminar un suscriptor de OpenManage Mobile:

1. Haga clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Móvil**.
2. Seleccione la casilla de verificación correspondiente al suscriptor y haga clic en **Eliminar**.
3. Cuando se lo solicite, haga clic en **Sí**.

Tareas relacionadas

Activación o desactivación de notificaciones de alerta de OpenManage Mobile en la página 175
Activación o desactivación de suscriptores de OpenManage Mobile en la página 175
Eliminación de un suscriptor de OpenManage Mobile en la página 175
Visualización del estado del servicio de notificación de alertas en la página 176

Información relacionada

Configuración de OpenManage Mobile en la página 174
Eliminación de un suscriptor de OpenManage Mobile en la página 175

Visualización del estado del servicio de notificación de alertas

OpenManage Enterprise reenvía las notificaciones de alerta a los suscriptores de OpenManage Mobile a través de su respectivo servicio de notificación de alertas de la plataforma del dispositivo. Si el suscriptor de OpenManage Mobile no pudo recibir notificaciones de alerta, puede comprobar el **Estado del servicio de notificación** para solucionar problemas con la entrega de las notificaciones de alerta.

Para ver el estado del servicio de notificación de alertas, haga clic en **Configuración de la aplicación** > **Móvil**.

Tareas relacionadas

Visualización del estado del servicio de notificación de alertas en la página 176

Información relacionada

Configuración de OpenManage Mobile en la página 174
Eliminación de un suscriptor de OpenManage Mobile en la página 175
Visualización del estado del servicio de notificación de alertas en la página 176

Estado del servicio de notificación

En la siguiente tabla se proporciona información sobre el **Estado del servicio de notificación** que se muestra en la página **Configuración de la aplicación** > **Móvil**.

Tabla 29. Estado del servicio de notificación

Icono de estado	Descripción del estado
	El servicio está ejecutando y operando con normalidad. **NOTA:** Este estado del servicio solo refleja las comunicaciones exitosas con el servicio de notificación de la plataforma. Si el dispositivo del suscriptor no está conectado a Internet o a un servicio de datos móviles, las notificaciones no se entregarán hasta que la conexión se restaure.
	El servicio experimenta un error al entregar un mensaje que puede ser de naturaleza temporal. Si el problema persiste, siga los procedimientos de solución de problemas o póngase en contacto con el servicio de soporte técnico.
	El servicio experimenta un error al entregar un mensaje. Siga los procedimientos de solución de problemas o póngase en contacto con el servicio de soporte técnico si es necesario.

Visualización de información acerca de los suscriptores de OpenManage Mobile

Después de que un usuario de OpenManage Mobile agrega correctamente OpenManage Enterprise, el usuario se agrega a la tabla **Suscriptores móviles** en OpenManage Enterprise. Para ver información acerca de los suscriptores móviles, en OpenManage Enterprise, haga clic en **Configuración de aplicación** > **Móvil**.

También puede exportar la información acerca de los suscriptores móviles a un archivo .CSV mediante la lista desplegable **Exportar**.

Información para suscriptores de OpenManage Mobile

En la tabla siguiente se proporciona información sobre la tabla **Suscriptores móviles** que aparece en la página **Configuración de la aplicación** > **Móvil**.

Tabla 30. Información para suscriptores de OpenManage Mobile

Campo	Descripción
HABILITADO	Seleccione o anule la selección de la casilla de verificación y, a continuación, haga clic en **Activar** o **Desactivar** respectivamente para activar o desactivar las notificaciones de alerta a un suscriptor de OpenManage Mobile.
ESTADO	Muestra el estado del suscriptor e indica si OpenManage Enterprise puede enviar correctamente notificaciones de alerta al servicio de reenvío de alertas.
MENSAJE DE ESTADO	Descripción del estado del mensaje de estado.
NOMBRE DE USUARIO	Nombre del usuario de OpenManage Mobile.
IDENTIFICACIÓN DEL DISPOSITIVO	Identificador único del dispositivo móvil.
DESCRIPCIÓN	Descripción del dispositivo móvil.
FILTRO	Los filtros son políticas que el suscriptor configuró para las notificaciones de alerta.
ÚLTIMO ERROR	La fecha y hora del último error ocurrido durante el envío de una notificación de alerta al usuario de OpenManage Mobile.
ÚLTIMO PUSH	La fecha y hora en que la última notificación de alerta se envió correctamente desde OpenManage Enterprise al servicio de reenvío de alertas.
ÚLTIMA CONEXIÓN	La fecha y hora de la última vez que el usuario accedió a OpenManage Enterprise a través de OpenManage Mobile.
REGISTRO	La fecha y hora en que el usuario agregó OpenManage Enterprise en OpenManage Mobile.

Solución de problemas de OpenManage Mobile

Si OpenManage Enterprise no se puede registrar con el servicio de reenvío de mensajes o no se pueden reenviar satisfactoriamente las notificaciones, puede usar las siguientes soluciones:

Tabla 31. Solución de problemas de OpenManage Mobile

Problema	Motivo	Solución
OpenManage Enterprise no puede conectarse al servicio de reenvío de mensajes de Dell. [Código 1001/1002]	Se perdió la conectividad Internet (HTTPS) de salida.	Mediante un explorador web, compruebe si está disponible la conectividad a Internet de salida.

Tabla 31. Solución de problemas de OpenManage Mobile (continuación)

Problema	Motivo	Solución
		Si la conexión no está disponible, realice las siguientes tareas solución de problemas con la red: • Verifique si los cables de red están conectados. • Verifique la dirección IP y la configuración del servidor DNS. • Verifique si el servidor de seguridad está configurado para permitir el tráfico de salida. • Verifique si la red ISP está funcionando normalmente.
	Los valores proxy son incorrectos.	Configure el host proxy, el puerto, el nombre de usuario y la contraseña como corresponda.
	El servicio de reenvío de mensajes no está disponible temporalmente.	Espere a que el servicio esté disponible.
El servicio de reenvío de mensajes no se puede conectar a un servicio de notificación de la plataforma de dispositivo. [Código 100-105, 200-202, 211-212]	El servicio del proveedor de la plataforma no está disponible temporalmente para el servicio de reenvío de mensajes.	Espere a que el servicio esté disponible.
El testigo de comunicación del dispositivo ya no se registra en el servicio del proveedor de la plataforma. [Código 203]	La aplicación OpenManage Mobile ha sido actualizada, restaurada o desinstalada, o bien el sistema operativo del dispositivo se ha actualizado o restaurado.	Reinstale OpenManage Mobile en el dispositivo o siga los procedimientos de solución de problemas de OpenManage Mobile que se especifican en la *Guía del usuario de OpenManage Mobile* y vuelva a conectar el dispositivo a OpenManage Enterprise. Si el dispositivo ya no está conectado a OpenManage Enterprise, quite al suscriptor.
El servicio de reenvío de mensajes rechaza el registro de OpenManage Enterprise. [Código 154]	Se está usando una versión obsoleta de OpenManage Enterprise.	Actualice a una versión más reciente de OpenManage Enterprise.

Tareas relacionadas

Configuración de OpenManage Mobile en la página 174

Información relacionada

Configuración de OpenManage Mobile en la página 174

21

Otras descripciones de los campos y referencias

En este capítulo, se describen e indican definiciones sobre algunos de los campos que comúnmente se muestran en la interfaz gráfica de usuario (GUI) de OpenManage Enterprise. Además, aquí se describe cualquier otra información útil para futuras referencias.

Temas:

Programar referencia

- **Actualizar ahora**: se actualiza la versión de firmware y se genera una coincidencia con la versión disponible en el catálogo relacionado. Para que la actualización sea eficaz durante el siguiente reinicio del dispositivo, seleccione la casilla de verificación **Preparación para el próximo reinicio del servidor**.
- **Programar más tarde**: seleccione esta opción para especificar una fecha y hora para en que se deba actualizar la versión de firmware.

Definiciones de los campos de la línea base de firmware

- **CUMPLIMIENTO**: el estado de la condición de la línea base del firmware. Incluso si un dispositivo asociado con una línea base de firmware se encuentra en estado de condición crítico, la condición de la línea base se define a sí misma como crítica. Esto se denomina resumen del estado de la condición, que es igual al estado de la línea base que tiene alta gravedad. Para obtener más información sobre el estado de Resumen de condición, consulte las notas técnicas *ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.a GENERACIÓN Y POSTERIORES* en Dell TechCenter.
- **NOMBRE**: el nombre de la línea base de firmware. Haga clic en esta opción para ver el informe de cumplimiento de línea base en la página **Informe de cumplimiento**. Para obtener más información sobre la creación de una línea base de firmware, consulteCrear una línea de base de firmware o controladores en la página 79.
- **CATÁLOGO**: el catálogo de firmware al cual pertenece la línea base de firmware. Consulte Administrar catálogos de firmware y controladores en la página 76.
- **HORA DE ÚLTIMA EJECUCIÓN**: la hora en la cual el informe de cumplimiento de línea base se ejecutó por última vez. Consulte Comprobar el cumplimiento del firmware y los controladores de un dispositivo en la página 80.

Definiciones de los campos Programar trabajos

- **Ejecutar ahora** para iniciar el trabajo inmediatamente.
- **Ejecutar más tarde** para especificar una fecha y hora posteriores.
- **Ejecutar según el programa** para ejecutar repetidamente según la frecuencia seleccionada. Seleccione **Diariamente** y, a continuación, seleccione correctamente la frecuencia.

NOTA: De manera predeterminada, el reloj del programador de trabajos se restablece a las 00:00 todos los días. El formato de cron no considera la hora de creación del trabajo cuando se calcula la frecuencia del trabajo. Por ejemplo, si un trabajo se inicia a las 10:00, y se debe ejecutar cada 10 horas, la próxima vez que se ejecute el trabajo será a las 20:00. Sin embargo, la siguiente vez no será a las 06:00 del día siguiente, sino a las 00:00, ya que el reloj del programador se restablece a las 00:00 todos los días.

Categorías de alerta después de la reubicación de EEMI

Tabla de reubicaciones de EEMI

Tabla 32. Categorías de alerta en OpenManage Enterprise

Categoría anterior	Subcategoría anterior	Nueva categoría	Nueva subcategoría
Auditorías	Dispositivos	Condición del sistema	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Dispositivos	Auditorías	Usuarios
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Dispositivos
Configuración	Inventario	Configuración	Dispositivos
Configuración	Inventario	Configuración	Dispositivos
Configuración	Firmware	Configuración	Trabajos
Configuración	Firmware	Configuración	Trabajos
Varios	Trabajos	Configuración	Trabajos
Varios	Trabajos	Configuración	Trabajos
Varios	Trabajos	Configuración	Trabajos
Varios	Generic	Configuración	Generic

Tabla 32. Categorías de alerta en OpenManage Enterprise (continuación)

Categoría anterior	Subcategoría anterior	Nueva categoría	Nueva subcategoría
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Dispositivos	Configuración	Dispositivos
Varios	Dispositivos	Configuración	Dispositivos
Auditorías	Seguridad	Configuración	Seguridad
Auditorías	Seguridad	Configuración	Seguridad
Auditorías	Seguridad	Configuración	Seguridad

Sustitución del token en secuencias de comandos remotas y política de alerta

OpenManage Enterprise admite el uso de tokens para mejorar secuencias de comandos remotas y la creación de políticas de alertas.

Tabla 33. Tokens admitidos en OpenManage Enterprise

Tokens	Descripción
$IP	Dirección IP del dispositivo
$MSG	Mensaje
$DATE	Fecha
$TIME	Hora
$SEVERITY	Gravedad
$SERVICETAG	Etiqueta de servicio
$RESOLUTION	Resolución recomendada
$CATEGORY	Nombre de categorías de alertas
$ASSETTAG	Etiqueta de propiedad
$MODEL	Nombre del modelo

Flujo de depuración de servicio de campo

En OpenManage Enterprise, puede autorizar la depuración de la consola mediante la opción depuración el servicio de campo (FSD).

Mediante el uso de FSD, puede realizar las siguientes tareas:

- Permitir la activación y la copia de los registros de depuración
- Permitir la copia de los registros en tiempo real
- Permitir la creación de una copia de seguridad o la restauración de archivos de base de datos a VM.

Los temas a los que se hace referencia en cada tarea proporcionan instrucciones detalladas. Para activar FSD, realice las siguientes tareas:

1. Desbloquear la capacidad de FSD. Consulte Desbloquear la capacidad FSD en la página 182.

2. Instalar o conceder archivo DAT.ini firmado de FSD. Consulte Instalar o conceder un archivo DAT.ini firmado de FSD en la página 182.
3. Llamar FSD. Consulte Llamar FSD en la página 182.
4. Desactivar FSD. Consulte Desactivar FSD en la página 183.

Desbloquear la capacidad FSD

Puede desbloquear la capacidad de FSD a través de la pantalla TUI.

1. Vaya al menú principal TUI.
2. En la pantalla TUI, para utilizar la opción FSD, seleccione **Activar modo de depuración de servicio de campo (FSD)**.
3. Para generar una nueva solicitud de desbloqueo de FSD, en la pantalla **Funciones de FSD**, seleccione **Capacidades de desbloqueo de FSD**
4. Para determinar la duración de las capacidades de depuración que se solicitan, seleccione una fecha de inicio y de finalización.
5. En la pantalla **Escoger capacidades solicitadas de depuración**, seleccione una capacidad de depuración de una lista de capacidades de depuración exclusiva para la consola. En la esquina inferior derecha, seleccione **Generar**.

   NOTA: La capacidad de depuración que se admite actualmente es `RootShell`.

6. En la pantalla **Descargar archivo DAT**, vea las instrucciones y la dirección URL del recurso compartido donde ya existe el archivo DAT.ini.
7. Utilice un cliente externo para extraer el archivo DAT.ini desde la dirección URL del recurso compartido que se menciona en el paso 6.

   NOTA: El directorio de descarga de recursos compartidos es solo de lectura y solo admite un archivo DAT.ini a la vez.

8. Realice una de las siguientes tareas dependiendo de que si es un usuario externo o interno de Dell EMC:
   - Envíe el archivo DAT.in a un contacto de Dell EMC para obtener la firma si es un usuario externo.
   - Cargue el archivo DAT.ini en el centro de autenticación de depuración del servicio en terreno de Dell (FSDAF) y envíelo.
9. Espere a que sea devuelto un archivo DAT.ini firmado y aprobado de Dell EMC.

Instalar o conceder un archivo DAT.ini firmado de FSD

Asegúrese de que recibió el archivo DAT.ini, firmado y aprobado por Dell EMC.

NOTA: Una vez que Dell EMC aprueba el archivo DAT.ini, debe cargar el archivo en el servidor de la consola que generó el comando original de desbloqueo.

1. Para cargar un archivo firmado DAT.ini, en la pantalla **Funciones de FSD**, seleccione **Instalar/conceder archivo DAT firmado de FSD**.

   NOTA: El directorio de carga de recursos compartidos es solo de escritura y solo admite un archivo DAT.ini a la vez. El tamaño límite del archivo DAT.ini es de 4 KB.

2. En la pantalla **Cargar archivo DAT firmado**, siga las instrucciones sobre cómo cargar el archivo DAT.ini a una URL determinada de recurso compartido de archivos.
3. Utilice un cliente externo para cargar el archivo DAT.ini en una ubicación de recurso compartido.
4. En la pantalla **Cargar archivo DAT firmado**, seleccione **Cargué el archivo DAT de FSD**.

Si no hay errores durante la carga del archivo DAT.ini, se muestra un mensaje que confirma la instalación correcta del certificado. Para continuar, haga clic en **Aceptar**.

La carga del archivo DAT.ini puede fallar debido a cualquiera de las siguientes razones:

- La carga del directorio de recursos compartidos no tiene suficiente espacio en el disco.
- El archivo cargado DAT.ini no corresponde a la solicitud previa de la capacidad de depuración.
- No es válida la firma proporcionada por Dell EMC para el archivo DAT.ini.

Llamar FSD

Asegúrese de que el archivo DAT.ini sea firmado y devuelto por Dell EMC y de que se cargue en OpenManage Enterprise.

1. Con el fin de invocar una capacidad de depuración, en la pantalla **Funciones de FSD**, seleccione **Invocar capacidades de FSD**.
2. En la pantalla **Invocar capacidades de depuración solicitada**, seleccione una capacidad de depuración de una lista de capacidades de depuración que esté aprobada en el archivo DAT.ini firmado por Dell EMC. En la esquina inferior derecha, haga clic en **Invocar**.

   NOTA: La capacidad de depuración que se admite actualmente es `RootShell`.

Mientras se ejecuta el comando `invoke`, OpenManage Enterprise puede iniciar un demonio SSH. El cliente SSH externo se puede conectar con OpenManage Enterprise para fines de depuración.

Desactivar FSD

Después de invocar una capacidad de depuración en una consola, seguirá funcionando hasta que se haya reiniciado la consola o se haya detenido la capacidad de depuración. De lo contrario, excede la duración que se determina a partir de la fecha de inicio y finalización.

1. Para detener las capacidades de depuración, en la pantalla **Funciones de FSD**, seleccione **Desactivar capacidades de depuración**.
2. En la pantalla **Desactivar capacidades de depuración invocadas**, seleccione una capacidad o capacidades de depuración de una lista de capacidades de depuración que se invocan actualmente. En la esquina inferior derecha de la pantalla, seleccione **Desactivar**.

Asegúrese de detener cualquier demonio SSH o sesión SSH que estén utilizando actualmente la capacidad de depuración.

Definiciones de campos de administración de catálogos

NOMBRE DEL CATÁLOGO: nombre del catálogo. Los catálogos incorporados no se pueden editar.

DESCARGAR: indica el estado de la descarga de catálogos de su carpeta del repositorio. Los estados son los siguientes: completos, en ejecución y con error.

REPOSITORIO: tipos de repositorios, tales como Dell.com, CIFS y NFS.

UBICACIÓN DEL REPOSITORIO: ubicación en la que se guardan los catálogos. Algunos ejemplos son Dell.com, CIFS y NFS. Además, indica el estado de finalización de un trabajo que se está ejecutando en el catálogo.

ARCHIVO DE CATÁLOGO: tipo de archivo de catálogo.

FECHA DE CREACIÓN: fecha en que se creó el archivo de catálogo.

Informes de base de cumplimiento del firmware o el controlador: dispositivos con estado de cumplimiento "Desconocido"

El estado de cumplimiento de firmware o controladores de los siguientes dispositivos de almacenamiento, redes e infraestructura hiperconvergente (HCI) en los informes de cumplimiento de la línea de base de firmware/controlador se muestra como desconocido, ya que el catálogo de firmware/controlador de Dell no es compatible con las actualizaciones de firmware o software para estos dispositivos.

Tabla 34. Informes de base de cumplimiento del firmware/controlador: “falsos positivos” en dispositivos compatibles

Categoría de dispositivos	Lista de dispositivos
Almacenamiento	• Serie SC • MD Series • Serie ME
Dispositivos de red en FX2, VRTX y el chasis M1000e	• Switches F10 • IOA (agregadores de entrada/salida) • IOM (módulos de entrada/salida)
Dispositivos hiperconvergentes (HCI)	• VXRail • Serie XC

Tabla 34. Informes de base de cumplimiento del firmware/controlador: "falsos positivos" en dispositivos compatibles (continuación)

Categoría de dispositivos	Lista de dispositivos
Los dispositivos se pueden actualizar mediante el Dell Update Package (DUP) del dispositivo individual, pero no se admiten directamente en el catálogo de Dell	• Motor de fabric MX9116n • Switch Ethernet MX5108n • PowerEdge MX5000s
Dispositivos que no se pueden actualizar mediante el catálogo de Dell ni el DUP individual **NOTA:** Para actualizar el firmware/controlador de estos dispositivos, consulte la guía de instalación del dispositivo correspondiente.	• Módulo de expansión de Fabric MX7116n • PTM de 25 GbE de PowerEdge MX

NOTA: Para obtener la lista completa de los dispositivos de las series SC, MD, ME y XC, consulte https://topics-cdn.dell.com/pdf/dell-openmanage-enterprise_compatibility-matrix2_en-us.pdf

Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge

Para cubrir una variedad de modelos de servidores, ahora se hace referencia a los servidores PowerEdge mediante la convención de nomenclatura genérica y no mediante su generación.

En este tema se explica cómo identificar la generación de un servidor PowerEdge al que se hace referencia utilizando la convención de nomenclatura genérica.

Ejemplo:

El modelo del servidor R740 es un sistema de rack que cuenta con dos procesadores de la 14.ª generación de servidores con procesadores Intel. En la documentación de, para referirse a R740, se utiliza el servidor **YX4X** con la convención de nomenclatura genérica y estas siglas hacen referencia a lo siguiente:

- La letra **Y** (alfabética) se utiliza para indicar los siguientes factores de forma de servidor:
  - **C** = Nube, nodos de servidor modular para entornos a gran escala
  - **F** = Flexible, sleds basados en rack para un gabinete FX2/FX2s basado en rack
  - **M** o **MX*** = Modular, servidores blade para el gabinete modular MX7000, M1000e o VRTX
  - **R** = Servidores de montaje en rack
  - **T** = Servidores en torre
- La letra **X** (dígito) señala la clase (número de procesadores) del servidor.
- El dígito **4** indica la generación del servidor.
- La letra **X** (dígito) señala la marca del procesador.

Tabla 35. Convención de nomenclatura de servidores PowerEdge junto con ejemplos

Servidores YX3X	Sistemas YX4X
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540