Dell EMC OpenManage Enterprise, versión 3.1

Guía del usuario

DELL EMC

Notas, precauciones y advertencias

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

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

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

2019 - 02

Rev. A01

Tabla de contenido

1

Acerca de Dell EMC OpenManage Enterprise

OpenManage Enterprise es una aplicación de administración y monitoreo de sistemas que ofrece una vista integral de los servidores, los chasis, el almacenamiento y los switch de red de Dell EMC en la red empresarial. Con OpenManage Enterprise, una aplicación web que permite administrar uno o varios sistemas, es posible:

- Detectar y administrar dispositivos en un entorno de centro de datos.
- Crear y administrar usuarios de OpenManage.
- Agrupar y administrar dispositivos.
- Supervisar la condición de los dispositivos.
- Administrar las versiones del firmware de los dispositivos y realizar actualizaciones de sistema y tareas remotas.
- Crear e implementar plantillas de configuración de dispositivos.
- Crear y asignar grupos de identidades y realizar implementaciones sin estado en dispositivos de destino.
- Crear líneas de base de cumplimiento de la configuración y reparar dispositivos
- Ver y administrar alertas del sistema y políticas de alerta.
- Ver inventario de hardware e informes de cumplimiento.
- Supervisar e informar la garantía y las licencias.

NOTA: 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 roles que limita el acceso a las configuraciones de la consola y a las acciones del dispositivo.
- 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:

- Implementación y administración de OpenManage Enterprise
- Configurar OpenManage Enterprise con interfaz de usuario de texto
- Detección de dispositivos para la supervisión o administración
- Administración de dispositivos
- Supervisión de dispositivos mediante el panel de OpenManage Enterprise
- Organizar los dispositivos en grupos
- Administrar el firmware del dispositivo
- Visualización y configuración de dispositivos
- Supervisión de alertas de dispositivos
- Visualizar las alertas archivadas
- Visualización de información de garantía del dispositivo
- Administrar las plantillas de configuración de dispositivos
- Administración del cumplimiento de la configuración del dispositivo
- Administrar plantillas de línea base de cumplimiento
- Administrar registros de auditoría
- Administración de los ajustes del servidor OpenManage Enterprise
- Ejecución de un trabajo de inventario ahora
- Administración de la garantía del dispositivo
- Informes
- Administración de archivos de MIB
- Privilegios de usuario de OpenManage Enterprise basados en el rol

- Integración de servicios de directorio en OpenManage Enterprise

Temas:

- Novedades de esta versión
- Otra información útil
- Cómo ponerse en contacto con Dell EMC
- Licencia de administración de configuración de servidor de OpenManage

Novedades de esta versión

- Capacidad de reenviar los registros de auditoría para realizar una supervisión remota mediante servidores de Syslog.
- Compatibilidad con los servidores Dell PowerEdge de 14.ª generación más recientes.
- Mejoras:
  - Disponibilidad de categorías de alerta adicionales para crear políticas de alerta.
  - Configuración de seguridad mejorada de SMB para admitir la firma de bloque de mensajes del servidor.
  - Uso de recursos compartidos de red CIFS seguros para realizar actualizaciones de firmware, mejoras y correcciones de errores durante un trabajo de actualización de firmware.

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
Dell EMC OpenManage Enterprise Support Matrix (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 **Manuales y documentos** para tener acceso a estos documentos.
Dell EMC OpenManage Enterprise Readme (archivo Léame de Dell EMC OpenManage Enterprise)	Permite obtener información sobre problemas conocidos y soluciones alternativas en OpenManage Enterprise.	
Dell EMC OpenManage Mobile User's Guide (Guía del usuario de Dell EMC OpenManage Mobile)	Proporciona información acerca de la instalación y el uso de la aplicación OpenManage Mobile.	
Dell EMC Repository Manager User's Guide (Guía del usuario de administrador de repositorios de Dell EMC)	Proporciona información sobre el uso de Repository Manager para administrar las actualizaciones del sistema	
Dell EMC OpenManage Enterprise and OpenManage Enterprise - Modular Edition RESTful API Guide (Guía de API RESTful de OpenManage Enterprise y OpenManage Enterprise - Edición Modular)	Permite obtener información sobre la integración de OpenManage Enterprise mediante las API de la transferencia representativa de estado (REST) y también incluye ejemplos referidos al uso de las API de REST para realizar tareas comunes.	
Dell EMC SupportAssist Enterprise User's Guide (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 administración de configuración de servidor de OpenManage

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

La licencia de *administración de configuración de servidor de OpenManage* 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 EnterpriseSupervisiónInformesInforme de licencia** y luego haga clic en **Ejecutar**. Consulte Ejecutar informes.

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 *administración de configuración de servidor de OpenManage* está instalada en un servidor de destino, puede usar la función de administración de configuración de servidor en dicho servidor.

Licencia de administración de configuración de servidor de OpenManage: servidores admitidos

Puede implementar la licencia de *administración de configuración de servidor de OpenManage* en los siguientes servidores PowerEdge:

- Servidores de 13<1>a</1> generación (13G) que tienen las versiones de firmware 2.50.50.50 de iDRAC8 o posteriores. Las versiones IDRAC de 13G también son compatibles para admitir las versiones iDRAC7 (12G).
- Servidores de 14<1>a</1> generación (14G) que tienen las versiones de firmware 3.10.10.10 de iDRAC9 o posteriores.

Adquisición de la licencia de administración de configuración de servidor de OpenManage

Puede adquirir la licencia de *administración de configuración de servidor de OpenManage* 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 integrado para ver la lista de dispositivos supervisados por OpenManage Enterprise y sus licencias. Haga clic en **OpenManage EnterpriseSupervisiónInformesInforme de la licencia**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

Puede verificar si la licencia de *administración de configuración de servidor de OpenManage* 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

Para ver la versión más reciente del servidor de OpenManage Enterprise instalado:

- Haga clic en el símbolo **i** en la esquina superior derecha que normalmente se muestra en todas las páginas de OpenManage Enterprise.
- Haga clic en **Configuración de aplicación** > **Actualización de consola**.

NOTA: Para ver si existe alguna versión más reciente de OpenManage Enterprise disponible, consulte Comprobación y actualización de la versión de OpenManage Enterprise. Asimismo, consulte las *Notas de la versión OpenManage Enterprise* disponibles en el sitio de soporte técnico.

2

Características de seguridad en OpenManage Enterprise

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

- Acceso basado en funciones que limita el acceso a la configuración y las acciones del dispositivo.
- Dispositivo 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 (HTTP).

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:

- **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 se sesión único (SSO) se puede usar solo hasta que se inicia sesión en el dispositivo.**
- **Las acciones que se ejecutan en los dispositivos requieren una cuenta con privilegios en el dispositivo.**

Información relacionada

Implementación y administración de OpenManage Enterprise

Temas:

Privilegios de usuario de OpenManage Enterprise basados en el rol

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. Este se conoce como Control de acceso basado en roles (RBAC). Se trata de una lista común de RBAC para los usuarios según sus roles y las funciones de OpenManage Enterprise. Sin embargo, cuando es necesario, se proporciona una lista de RBAC de usuario a nivel de tareas en las secciones respectivas para una referencia rápida. Por lo tanto, en la consola se aplica uno de los roles por cuenta. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte Administración de usuarios de OpenManage Enterprise.

Tabla 2. Privilegios de usuario basados en roles en OpenManage Enterprise

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Administrador	Administrador de dispositivos	Lector
Ejecutar informes	S	S	S
Ver	S	S	S
Administrar plantillas	S	S	N
Administrar la línea de base	S	S	N

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Administrador	Administrador de dispositivos	Lector
Configurar el dispositivo	S	S	N
Actualizar el dispositivo	S	S	N
Administrar los trabajos	S	S	N
Crear supervisión de políticas	S	S	N
Implementar un SO	S	S	N
Control de alimentación	S	S	N
Administrar informes	S	S	N
Actualizar inventario	S	S	N
Configurar el dispositivo de OpenManage Enterprise	S	N	N
Administrar la detección	S	N	N
Administrar los grupos	S	N	N
Configurar la seguridad	S	N	N
Administrar capturas	S	N	N

Tareas relacionadas

Implementación y administración de OpenManage Enterprise

Referencia relacionada

Tipos de roles de usuario en OpenManage Enterprise

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).**
- **La función de inicio se sesión único (SSO) se puede usar solo hasta que se inicia sesión en el dispositivo.**
- **Las acciones que se ejecutan en los dispositivos requieren una cuenta con privilegios en el dispositivo.**

Tabla 3. 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. · 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

El usuario con este rol...	Tiene los siguientes privilegios del usuario
Administrador de dispositivos (DM) **NOTA: Los DM pueden compartir los permisos necesarios para las tareas y las políticas que crean entre sí. Este uso compartido se produce con una superposición completa con los grupos de dispositivos que se encuentran en la tarea o política de lectura y aquellos asignados al DM. Si el DM pierde la superposición completa con los grupos que se encuentran en la tarea o política, el DM ya no podrá ejecutarla ni editarla, a menos que esta superposición se restaure.**	• Obtiene solamente permisos de dispositivos otorgados por el administrador. Todos los demás permisos son fijos. • Ejecute tareas, políticas y otras acciones en los dispositivos asignados por el administrador. • No puede eliminar ni modificar grupos. **NOTA: No se pueden asignar grupos a los usuarios con privilegios de administrador de dispositivos (DM).**
Lector	• 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 DM, el DM tiene los mismos privilegios como observador.**
- **Un cambio en el rol de usuario no afectará al usuario que haya iniciado sesión. Los cambios tienen efecto solo después del siguiente inicio de sesión del usuario.**
- **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

Implementación y administración de OpenManage Enterprise

Información relacionada

Privilegios de usuario de OpenManage Enterprise basados en el rol

3

Implementación y administración de OpenManage Enterprise

Dell EMC OpenManage Enterprise se proporciona como un servidor que puede implementar 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 Comprobación y actualización de la versión de OpenManage Enterprise. 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.

Referencia relacionada

Tipos de roles de usuario en OpenManage Enterprise
Mapa de procesos para la comprobación y actualización de la versión de OpenManage Enterprise
Descripción general de interfaz gráfica de usuario de OpenManage Enterprise
Características de seguridad en OpenManage Enterprise

Información relacionada

Privilegios de usuario de OpenManage Enterprise basados en el rol

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

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	16 GB	16 GB
Procesadores	8 núcleos en total	4 núcleos en total
Unidad de disco duro	200 GB	20 GB

Requisitos mínimos del sistema para implementar OpenManage Enterprise

Tabla 5. Requisitos mínimos

Detalles	Requisitos mínimos

Hipervisores compatibles	• Versiones de VMware vSphere:
	  • vSphere ESXi 6.5
	  • vSphere ESXi 6.0
	  • vSphere ESXi 5.5
	• Microsoft Hyper-V compatible en:
	  • Windows Server 2016
	  • Windows Server 2012 R2
	• KVM compatible en:
	  • Red Hat Enterprise Linux 7.2
	  • Red Hat Enterprise Linux 7.0
	  • Red Hat Enterprise Linux 6.5

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
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 Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. Descargue el archivo `openmanage_enterprise_ovf_format.zip` desde el sitio de soporte y extraiga el archivo en una ubicación a la que pueda acceder VMware vSphere Client. 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 **File 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 **Next** (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

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 hacia 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 y versiones anteriores. 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 **AcciónNuevaMáquina virtual**.
4. En la página **Especificar nombre y ubicación**, seleccione el nombre de la VM y una ubicación de almacenamiento de forma adecuada para su entorno.
5. Vaya a la página **Especificar Generación** y seleccione **1.ª generación**. OpenManage Enterprise no es compatible con la 2.ª generación.

   NOTA: Asegúrese de que se haya asignado 16 GB como la memoria. Se puede encender la memoria dinámica, pero para obtener el rendimiento óptimo, se recomienda que deje la opción "deshabilitada".
6. En la página **Configuración de redes**, asegúrese de que el adaptador de red esté conectado a la red. Si se establece en 'No Conectado', OME no funcionará correctamente durante el primer reinicio y requiere la reimplementación si reaparece esta situación.
7. En la página **Conectar disco duro virtual**, seleccione **Usar una unidad de disco virtual existente** y, luego, vaya al archivo VHD que copió en el Paso 1.
8. Complete las instrucciones que aparecen en pantalla.
9. Abra la configuración de la VM que se creó recientemente.

Implementar OpenManage Enterprise en un host de Hyper-V 2016

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 hacia la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
2. Inicie el administrador de Hyper-V.
3. Seleccione el host y seleccione **Acción** > **Importar máquina virtual**.
4. Seleccione la carpeta que contiene el dispositivo virtual OpenManage Enterprise, que incluye instantáneas, unidades virtuales, VM y archivos de importación. Haga clic en **Siguiente**.
5. En la página **Seleccionar máquina virtual**, seleccione la máquina virtual que desee importar (solo hay una opción disponible) y, a continuación, haga clic en **Siguiente**.
6. En la página **Elegir tipo de importación**, seleccione **Copiar la máquina virtual** y, a continuación, haga clic en **Siguiente**.
7. En la página **Elegir destino**, conserve los valores predeterminados o seleccione la ubicación de la VM, la instantánea y la paginación inteligente.
8. Haga clic en **Siguiente**.
9. En la página **Elegir carpetas de almacenamiento**, conserve los valores predeterminados o haga clic en **Examinar** y seleccione la ubicación de las unidades virtuales y, a continuación, haga clic en **Siguiente**.
10. En la página **Resumen**, revise las opciones que seleccionó en páginas anteriores y, a continuación, haga clic en **Finalizar** para implementar el dispositivo virtual OpenManage Enterprise en el host de Hyper-V.
11. Una vez que se implemente el dispositivo virtual OpenManage Enterprise, selecciónelo y, a continuación, haga clic en **Iniciar** en **Acciones**.

NOTA: El archivo del dispositivo OpenManage Enterprise también se puede implementar mediante el uso de un entorno KVM compatible.

Implementación de OpenManage Enterprise utilizando una máquina virtual basada en kernel

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 **ArchivoPropiedades**.
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 **ArchivoNuevo**.
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.

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.

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. Para detectar los dispositivos, haga clic en **Detectar dispositivos**.

NOTA: Si se ingresan credenciales incorrectas de inicio de sesión de OpenManage Enterprise, la cuenta de OpenManage Enterprise se bloqueará y no podrá iniciar sesión hasta que termine el período de bloqueo. De manera predeterminada, la duración del bloqueo es de 900 segundos. Para cambiar este período, consulte Establecimiento de las propiedades de seguridad de inicio de sesión.

Configurar OpenManage Enterprise con interfaz de usuario de texto

La herramienta Text User Interface (Interfaz de usuario de texto, TUI) proporciona una interfaz de texto para cambiar la contraseña de administrador, ver el estado del dispositivo y la configuración de la red, configurar parámetros del sistema de red y habilitar la solicitud de depuración de servicio de campo.

NOTA: Para navegar en la interfaz TUI, utilice las teclas de flecha o presione Pestaña para avanzar a la siguiente opción de la TUI y, a continuación, presione Mayús + Tab para a las opciones anteriores. Presione Intro para seleccionar una opción. La barra espaciadora cambia el estado de una casilla de verificación.

1. Antes de iniciar sesión en la TUI, acepte el EULA cuando se le solicite.
   a) En la pantalla **Cambiar la contraseña del administrador**, ingrese la nueva contraseña y confírmela.

      NOTA: La primera vez, debe cambiar la contraseña en la pantalla TUI.

   b) Utilice las teclas de flecha o presione **Pestaña** para seleccionar **Aplicar**.
   c) Cuando se le solicite confirmación, seleccione **Sí** y, a continuación presione **Intro**.

   Ahora puede configurar OpenManage Enterprise mediante la TUI. En la pantalla TUI puede ver las siguientes opciones:

   - **Cambiar la contraseña del administrador**
   - **Ver estado del dispositivo actual**

- **Ver la configuración de red actual**
- **Establecer parámetros del sistema de red**
- **Activar modo Depuración de servicio de campo (FSD)**
- **Reiniciar el dispositivo**

  NOTA: Es probable que, después de ejecutar un comando para reiniciar los servicios, observe que la TUI muestra el siguiente mensaje: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439]`. Este problema de bloqueo de software probablemente se produce como consecuencia de una 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 registro de depuración**
  - **Habilitar registros de depuración**
  - **Desactivar registros de depuración**
  - **Activar retención de SCP**
  - **Desactivar retención de SCP**
- **Reiniciar servicios**

2. Para confirmar la contraseña actual del administrador del dispositivo, seleccione **Cambiar la contraseña del administrador** y, a continuación, ingrese la contraseña. Presione **Pestaña** y seleccione **Continuar**.
3. En la pantalla TUI:
   a) Para ver el estado del dispositivo y los estados y las direcciones IPv4 e IPv6, seleccione **Estado actual del servidor**.
   b) Para configurar la interfaz de red, seleccione **Establecer parámetros del sistema de red**.
   En la pantalla **Configurar interfaz de red**, para activar la IPv4 o IPv6, o ambos, presione **Intro**. Seleccione **Aplicar**.

   NOTA:
   - **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.**
   - **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.**
   - **Para realizar las operaciones de escritura en TUI, asegúrese de ingresar la contraseña de administrador y, a continuación, configure IPv4 o IPv6.**
   - **Para configurar IPv6, asegúrese de que ya esté configurado por un vCenter Server.**
   - **En un entorno IPv6, cuando se configura un anuncio de enrutador para una configuración sin estado de varias IP de IPv6 en un puerto, el iDRAC admite un máximo de 16 direcciones IP. En tal caso, OpenManage Enterprise solo muestra la IP descubierta por última vez y utiliza esa IP como la interfaz fuera de banda para iDRAC.**
   - **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.**

   c) Para activar la depuración de la consola, seleccione **Activar modo Depuración de servicio de campo (FSD)**. Consulte Flujo de depuración de servicio de campo.
   d) Para recopilar los registros de depuración de la aplicación, las tareas de supervisión, los eventos y el historial de ejecución de tareas, seleccione **Configurar registro de depuración**. Además, para recopilar los archivos de la plantilla .XML, seleccione la opción **Habilitar retención SCP** en **Configurar registro de depuración**. Puede descargar los registros de depuración haciendo clic en **SupervisarRegistros de auditoríaExportarExportar registros de consola** en OpenManage Enterprise.
   e) Para reiniciar OpenManage Enterprise, seleccione **Reiniciar el dispositivo**.

Configurar OpenManage Enterprise

Si está iniciando sesión en OpenManage Enterprise por primera vez, aparece la página **Bienvenido a OpenManage Enterprise**. Para configurar los ajustes básicos, haga clic en **Configuración inicial** e ingrese o seleccione los siguientes datos en el cuadro de diálogo:

1. En el menú descendente **Zona horaria**, seleccione una zona horaria. Haga clic en **Aplicar** para guardar la zona horaria seleccionada. Para establecer la zona horaria con el valor predeterminado, haga clic en **Descartar**. Después de actualizar la zona horaria, se cierran las sesiones de todos los usuarios activos de OpenManage Enterprise.
2. Si desea utilizar el servidor NTP para sincronización de tiempo, seleccione la casilla de verificación **Usar servidor NTP**.

   NOTA: Cuando se actualiza la configuración del servidor NTP, se cierran automáticamente las sesiones de los usuarios actualmente conectados a OpenManage Enterprise.
3. Para la sincronización de tiempo, ingrese la dirección IP o el nombre de host en **Dirección de servidor NTP principal** y **Dirección de servidor NTP secundaria** (opcional).
4. Si desea configurar un servidor proxy para la comunicación externa, seleccione la casilla de verificación **Usar configuración de proxy HTTP**.
5. En la casilla **Dirección IP del servidor**, ingrese la dirección IP o el nombre del host del servidor proxy.
6. En la casilla **Puerto**, ingrese el número de puerto del servidor proxy.
7. Si el servidor proxy requiere credenciales para iniciar sesión, seleccione la casilla de verificación **Usar credenciales de proxy**, ingrese nombre de usuario y contraseña.
8. Haga clic en **FINALIZAR**.

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 6. Consideraciones de escalabilidad y rendimiento de OpenManage Enterprise

Tareas	Frecuencia recomendada para ejecutar las tareas	¿Tareas preestablecidas?	Número máximo de dispositivos recomendados por tarea
Detección	Una vez al día para entornos con cambios de red frecuentes.	No	4000/tarea
Inventario	OpenManage Enterprise ofrece una tarea prestablecida que actualiza automáticamente el inventario una vez al día.	Sí. Puede desactivar esta función.	Dispositivos monitoreados por OpenManage Enterprise.
Garantía	OpenManage Enterprise ofrece una tarea prestablecida que actualiza automáticamente la garantía una vez al día.	Sí. Puede desactivar esta función.	Dispositivos monitoreados por OpenManage Enterprise.
Sondeo de la condición	Cada una hora	Sí. Puede cambiar la frecuencia.	Not applicable
Actualización del firmware	Según sea necesario		100/tarea
Inventario de configuración	Según sea necesario		50/línea de base

Protocolos y puertos admitidos en OpenManage Enterprise

Protocolos y puertos admitidos en Management Stations

Tabla 7. Protocolos y puertos admitidos por OpenManage Enterprise en Management Stations

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. Redirigirá a los usuarios a HTTPS.
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 las plantillas de configuración del dispositivo, cargar registros de TSR y de diagnóstico y para descargar DUP de firmware.
				Dispositivo OpenManage Enterprise	Salida	Recurso compartido de CIFS	Para importar catálogos de firmware desde el recurso compartido CIFS.
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.

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
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.
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 8. 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	Nodos administrados por Linux	Solo para detección en el sistema operativo Linux.
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, y para la administración de CMC.
623	IPMI/ RMCP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	Acceso a IPMI mediante LAN

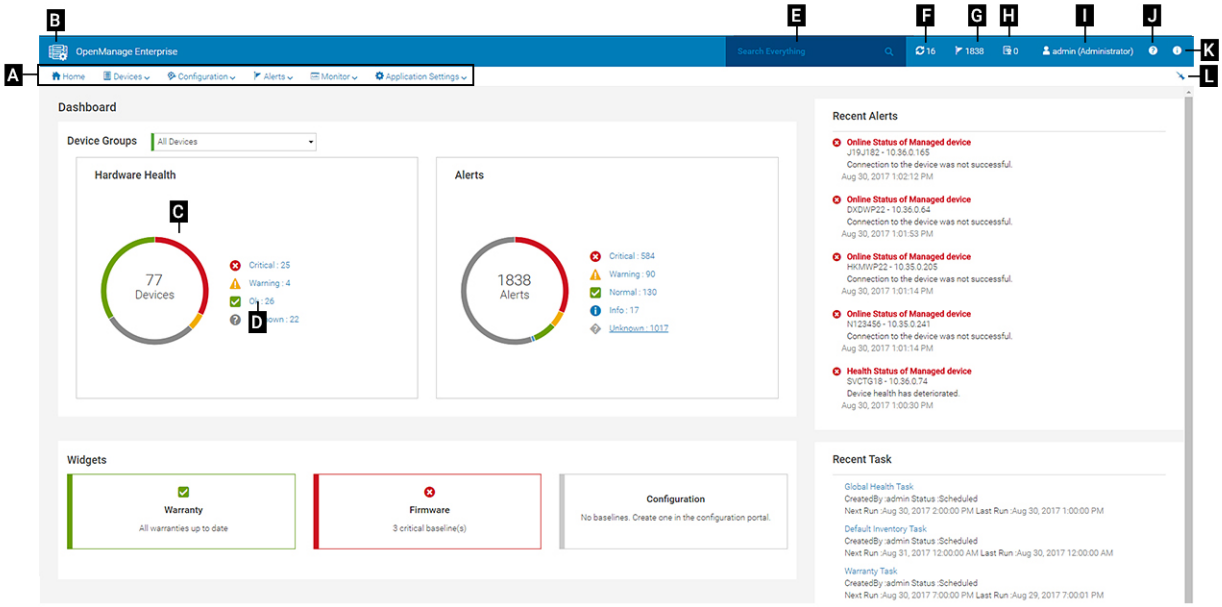
* El puerto se puede configurar hasta 499 sin incluir los números de puerto que ya están asignados.

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.

5

Descripción general de interfaz gráfica de 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. 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 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 vínculos a las características que permiten a los administradores ver el panel (**Inicio**), administrar los dispositivos (**Dispositivos**), administrar las líneas base del firmware, las plantillas y las líneas base de cumplimiento de la configuración (**Configuración**), crear y almacenar las alertas (**Alertas**) y, luego, ejecutar trabajos, detectar, recopilar 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 visión general 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 Visualización y configuración de dispositivos.
- D: Los símbolos utilizados para indicar el estado de los dispositivos. Consulte Estados de los dispositivos.
- E: en el cuadro **Buscar todo**, ingrese lo que esté bajo supervisión y que se pueda mostrar en OpenManage Enterprise para ver los resultados como la IP del dispositivo, el nombre del trabajo, el nombre de grupo, la línea de base del firmware y los datos de la garantía. 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 ".
  - El texto ingresado como criterio de búsqueda distingue entre mayúsculas y minúsculas.
  - No se admiten los siguientes caracteres comodines: `#`, `@`, `%`, `-`, `:`, `=`, `&`, `$`, `+`, `|`, `/`, `.`, `_`, `(` ni `)`.

- 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, la actualización de firmware, 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. Haga clic en Actualizar.
- G: número de eventos generados en los registros de alerta. 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. 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: número de dispositivos cuyo estado de garantía es crítico y requiere atención inmediata. Haga clic para ver las alertas del sistema de cada categoría. Para activar esta función, active la configuración de la garantía. 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 Privilegios de usuario de OpenManage Enterprise basados en el rol. 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. 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, el estado de la conexión, el estado de alimentación y 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 acerca del dispositivo, el trabajo, el inventario, la línea de base del firmware, la aplicación de administración, la consola virtual, etc. 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 servidor está disponible alguna versión actualizada de OpenManage Enterprise, recibirá un aviso para actualizar la versión inmediatamente haciendo clic en **Actualizar ahora**. Los usuarios con todos los privilegios de OpenManage Enterprise (administrador, administrador de dispositivos y lector) 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 Comprobación y actualización de la versión de OpenManage Enterprise.

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 la lista de trabajos.

Información relacionada

Implementación y administración de OpenManage Enterprise

6

Portal de inicio de OpenManage Enterprise

Si hace clic en **OpenManage EnterpriseInicio**, 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 widgets indica los estados acumulados de la garantía, el cumplimiento de firmware y el cumplimiento de la configuración de todos los dispositivos.

  Para obtener más información sobre las características en Widgets, consulte Supervisión de dispositivos mediante el panel de OpenManage Enterprise. 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 Supervisión de alertas de dispositivos y Utilización de trabajos para el control de dispositivos.
- Si se encuentra disponible una versión actualizada de OpenManage Enterprise, se alerta inmediatamente cuando haya una actualización disponible. Para actualizar, haga clic en **Actualizar ahora**. Para obtener más información acerca de la actualización de la versión de OpenManage Enterprise, consulte Comprobación y actualización de la versión de OpenManage Enterprise.
- 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 la lista de trabajos.

Temas:

Supervisión de dispositivos mediante el panel de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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**. Mediante la utilización de los datos de supervisión en tiempo real, en el panel se muestran la condición del dispositivo, el cumplimiento del firmware, la garantía, las alertas y otros aspectos de los dispositivos y grupos de dispositivos 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 y Organizar los dispositivos en grupos.

- Administrar el firmware del dispositivo
- Administración de alertas de dispositivos
- Detección de dispositivos
- Creación de informes
- Administración de los ajustes del servidor OpenManage Enterprise

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 Supervisión de alertas de dispositivos. 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 Visualización y configuración de dispositivos. Para filtrar los datos, haga clic en **Filtros avanzados**. Exporte los datos en formato Excel, CSV, HTML o PDF. Consulte Exportar todos los datos o aquellos seleccionados.

Para obtener más información sobre un gráfico de anillo, consulte Gráfico de anillo y Estados de los dispositivos. 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 Visualización y configuración de dispositivos.

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. Haga clic para ver más información en el cuadro de diálogo **Garantía**. Consulte Administrar la garantía del dispositivo utilizando el tablero de OpenManage Enterprise. Para obtener información sobre la administración de la garantía del dispositivo, consulte Administración de la garantía del dispositivo. Detenga el puntero del mouse sobre la sección **Garantía** para leer las definiciones sobre los símbolos utilizados en la sección.
- **Firmware**: muestra el estado de la condición de las líneas de base de cumplimiento del firmware creadas en OpenManage Enterprise. Si están disponibles, en esta sección se muestran las líneas base de firmware críticas y de aviso.
  - 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 el cuadro de diálogo **Firmware**.
  - Consulte Administrar las líneas base del firmware utilizando el tablero de OpenManage Enterprise.
  - 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 del dispositivo.
- **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 línea base de cumplimiento.

Administrar las líneas base del firmware utilizando el tablero de OpenManage Enterprise

En la página Panel de OpenManage Enterprise, en la sección **Widgets**, la sección **Firmware** muestra el número de líneas base de firmware que tienen uno o más dispositivos en estado de condición crítico. Consulte Estados de los dispositivos. Para obtener más información sobre la administración de firmware, consulte Administrar el firmware del dispositivo.

Para ver una lista de las líneas base, haga clic en **Firmware**. Para conocer las definiciones sobre los campos del cuadro de diálogo **Firmware**, consulte Definiciones de los campos de la línea base de firmware.

Administrar la garantía del dispositivo utilizando el tablero de OpenManage Enterprise

En la página Panel de OpenManage Enterprise, en la sección **Widgets**, la sección **Garantía** muestra el número de dispositivos cuya garantía está por caducar o ya ha caducado. Para obtener más información acerca de la administración de la garantía de un dispositivo, consulte Administración de la garantía del dispositivo.

Para ver una lista de las garantías que están por caducar, haga clic en **Garantía**. En la página **Garantía**, aparece la siguiente información:

- El estado, la etiqueta de servicio, el nombre del modelo y el tipo de los dispositivos.
- **TIPO DE GARANTÍA**:
  - **INICIAL**: la garantía sigue siendo válida mediante la garantía proporcionada cuando se adquirió por primera vez OpenManage Enterprise.
  - **EXTENDIDA**: la garantía se extiende porque caducó la duración de la garantía proporcionada cuando se adquirió por primera vez OpenManage Enterprise.
- **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.

Administrar líneas base de cumplimiento de los dispositivos a través del tablero de OpenManage Enterprise

En la página Panel de OpenManage Enterprise, en la sección **Widgets**, la sección **Configuración** muestra la cantidad de líneas base de cumplimiento de la configuración que no cumplen con las propiedades de la plantilla con la que se compara.

Para ver una lista de las líneas base de cumplimiento de la configuración que se desvían de las propiedades de la plantilla, haga clic en **Configuración**. En la página **Cumplimiento**:

- **CUMPLIMIENTO** indica el nivel de desviación de la línea base de cumplimiento de la configuración.
- **NOMBRE** indica el nombre de la línea de base de cumplimiento de configuración.
- **NOMBRE DE LA PLANTILLA** indica la plantilla de línea de base de cumplimiento con la cual se está comparando la línea de base.

Consulte Administración del cumplimiento de la configuración del dispositivo. Puede crear plantillas de línea base utilizando una plantilla de implementación, un dispositivo de referencia o mediante la importación desde un archivo. Consulte Administrar plantillas de línea base de cumplimiento.

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 Visualización y configuración de dispositivos.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos supervisados por OpenManage Enterprise. Haga clic en **OpenManage EnterpriseSupervisiónInformesInforme de la descripción general de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 Dell EMC Compellent
- **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.

  NOTA: La función Grupo de detección no es compatible con OpenManage Enterprise 3.0 ni versiones posteriores. Si creó grupos de detección en OpenManage Enterprise - Tech Release y actualizó a OpenManage Enterprise 3.1, todos los datos asociados se eliminarán después de la actualización y no se ejecutarán las tareas ni los trabajos asociados.

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: creados por el usuario 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.**

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 o eliminar un grupo estático de dispositivos y Crear o editar un grupo de dispositivos de consulta.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.

Tareas relacionadas

Eliminar dispositivos de OpenManage Enterprise
Actualizar el inventario de dispositivos
Actualizar el estado del dispositivo

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. 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 Supervisión de alertas de dispositivos.
- Para conocer el cumplimiento de la versión de firmware de un dispositivo en comparación con la versión del catálogo, consulte Administrar el firmware del dispositivo.
- 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.

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 Degradar , pero si el cumplimiento de un dispositivo en el grupo es Actualizar el nivel de cumplimiento de la línea base de firmware 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 9. 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

Administración de dispositivos

Si hace clic en **OpenManage EnterpriseDispositivosTodos los dispositivos**, puede ver los dispositivos y los grupos de dispositivos que administra OpenManage Enterprise. Los grupos de sistema son grupos predeterminados que se crean en OpenManage Enterprise cuando se envía y los grupos personalizados son los que crean los usuarios tales como administradores y administradores de dispositivos. Puede crear grupos secundarios en estos dos grupos principales. Para obtener información sobre las normas para los grupos principales-secundarios, consulte Grupos de dispositivos. En el panel de trabajo, en un gráfico de anillo se muestra de forma gráfica la condición y el número de dispositivos en el grupo seleccionado en el panel izquierdo. Para obtener más información sobre el gráfico de anillo, consulte Gráfico de anillo.

En la tabla dispuesta después del gráfico de anillo aparecen las propiedades de los dispositivos seleccionados en el panel izquierdo. Para ver las propiedades de un dispositivo y editar la configuración, haga clic en el nombre del dispositivo o la dirección IP en la lista. Para obtener más información sobre la lista de dispositivos, consulte Lista de dispositivos.

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.

NOTA: En la lista Dispositivos, haga clic en el nombre del dispositivo para ver los datos de configuración del dispositivo y, a continuación, editarlos. Para iniciar sesión en la aplicación de administración instalada en el dispositivo (por ejemplo, iDRAC), haga clic en la dirección IP. Consulte Visualización y configuración de dispositivos.

NOTA: Algunas de las tareas que están relacionadas con los dispositivos se pueden 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 la página Dispositivos <nombre del dispositivo>.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Puede seleccionar un máximo de 25 dispositivos por página y navegar por las páginas para seleccionar más dispositivos y realizar tareas. Puede realizar las siguientes tareas relacionadas con los dispositivos:

- Crear un grupo nuevo y agregar dispositivos. Consulte Adición de dispositivos a un nuevo grupo y Adición de dispositivos a un grupo existente.
- Eliminar un dispositivo de OpenManage Enterprise. Consulte Eliminar dispositivos de OpenManage Enterprise.
- Excluir un dispositivo de la supervisión de OpenManage Enterprise. Consulte Excluir dispositivos de OpenManage Enterprise.
- Actualizar la versión de firmware de un dispositivo. Consulte Actualización de la versión de firmware del dispositivo.
- Actualizar el inventario de hardware y software de los dispositivos seleccionados. Consulte Actualización del inventario de dispositivos.
- Recopilar los estados de funcionamiento más recientes de los dispositivos seleccionados.
- Incorporar dispositivos. Consulte Incorporación de dispositivos.
- Exportar los elementos en una lista de grupo de dispositivos en formato PDF, HTML y CSV. Consulte Exportación del inventario del grupo de dispositivos.
- Exportar datos sobre los dispositivos seleccionados o todos los dispositivos en la lengüeta Más acciones. Consulte Exportación de datos.
- Ver información completa y administrar un dispositivo. Consulte Visualización y configuración de dispositivos.
- Iniciar el iDRAC con la aplicación de administración Lifecycle Controller. Consulte Inicio de aplicación de administración (iDRAC) de un dispositivo.
- Iniciar la consola virtual. Consulte Iniciar la consola virtual.

Para las tareas relacionadas con grupos de dispositivos, consulte Organizar los dispositivos en grupos.

En la esquina superior derecha, en la sección **VÍNCULOS RÁPIDOS**, utilice los vínculos rápidos a las siguientes funciones de OpenManage Enterprise:

- Detección de dispositivos
- Ejecución de un trabajo de programa de inventario ahora
- Dispositivos excluidos globalmente de los resultados de detección

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. Para borrar las selecciones, haga clic en **Borrar selección**.

NOTA: Para obtener más información sobre los sucesos y los errores específicos que se muestran en la interfaz gráfica de usuario (GUI) o que se guardan en el registro para fines informativos, consulte la última *Guía de referencia de mensajes de error y sucesos para los servidores Dell EMC PowerEdge* disponible en el sitio de soporte técnico.

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 Visualización y configuración de dispositivos.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos supervisados por OpenManage Enterprise. Haga clic en **OpenManage EnterpriseSupervisiónInformesInforme de la descripción general de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 Dell EMC Compellent
- **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.

  NOTA: La función Grupo de detección no es compatible con OpenManage Enterprise 3.0 ni versiones posteriores. Si creó grupos de detección en OpenManage Enterprise - Tech Release y actualizó a OpenManage Enterprise 3.1, todos los datos asociados se eliminarán después de la actualización y no se ejecutarán las tareas ni los trabajos asociados.

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: creados por el usuario 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.**

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 o eliminar un grupo estático de dispositivos y Crear o editar un grupo de dispositivos de consulta.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.

Tareas relacionadas

Eliminar dispositivos de OpenManage Enterprise
Actualizar el inventario de dispositivos
Actualizar el estado del dispositivo

Crear o eliminar un grupo estático de dispositivos

En la página Todos los dispositivos, puede crear o editar grupos secundarios en el grupo estático principal. Para realizar estas tareas, debe tener los privilegios de usuario adecuados. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. Haga clic con el botón derecho del ratón en **Grupos estáticos** y, a continuación, haga clic en **Crear nuevo grupo estático**.
2. En el cuadro de diálogo **Asistente para crear grupo estático**, ingrese el nombre y la descripción 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 **Finalizar**.
   El grupo se crea y se coloca en el grupo principal en el panel izquierdo. Los grupos secundarios aparecen en sangría desde su grupo principal.

NOTA: No puede agregar dispositivos directamente en los grupos estáticos. Debe crear grupos estáticos secundarios y, a continuación, agregar los dispositivos en los grupos secundarios.

Para eliminar el grupo secundario de un grupo estático:

1. Haga clic con el botón secundario en el grupo estático y luego haga clic en **Eliminar**.
2. Cuando se le solicite, haga clic en **SÍ**. Se elimina el grupo y se actualiza la lista en grupo.

Crear o editar un grupo de dispositivos de consulta

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. Haga clic con el botón derecho del ratón en **Grupos de consulta** y, a continuación, haga clic en **Crear nuevo grupo de consulta**.
   Para conocer las definiciones de grupo estático o de consulta (dinámico), consulte Organizar los dispositivos en grupos.
2. En el cuadro de diálogo **Asistente para crear grupo de consulta**, ingrese un nombre y una descripción 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.
5. Haga clic en **Finalizar**.
   El grupo de consulta se crea y se coloca en el grupo principal del panel de la izquierda.
   NOTA: No puede agregar dispositivos directamente en los grupos de consultas. Debe crear grupos de consulta secundarios y, a continuación, agregar los dispositivos en los grupos secundarios.

   Para editar un grupo de consulta:

   a. En el panel izquierdo, haga clic con el botón derecho del mouse en el grupo secundario de consulta y haga clic en **Editar**.
   b. De manera alternativa, haga clic en el grupo secundario de consulta en el panel izquierdo. En el panel de trabajo se muestra una lista de dispositivos en el grupo. Haga clic en el vínculo **Editar** en la banda gris que aparece encima de la lista de dispositivos. Aparece el cuadro de diálogo **Asistente para crear grupo de consulta**.
   c. En el cuadro de diálogo **Asistente para crear grupo de consulta**, ingrese o seleccione los datos como se describe anteriormente en esta sección.

   Para eliminar el grupo secundario de un grupo de consulta:

   a. Haga clic con el botón secundario en el grupo de consulta y luego haga clic en **Eliminar**.
   b. Cuando se le solicite, haga clic en **SÍ**. Se elimina el grupo y se actualiza la lista en grupo.

Seleccionar los criterios de una consulta

Defina filtros cuando cree criterios de consulta para:

- Generación de informes personalizados. Consulte Creación de informes.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte Crear o editar un grupo de dispositivos de consulta.

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. El número de filtros predefinidos para cada consulta existente varía según el tipo de consulta. Por ejemplo, la consulta para **sistemas hipervisor** tiene 6 filtros predefinidos, mientras la consulta para **los conmutadores de red** tiene solo tres. Cuando se define una consulta, es posible definir un máximo de 20 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 Administrar registros de auditoría.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo
Editar una línea base de cumplimiento de configuración
Eliminar una línea base de cumplimiento de configuración

Cómo agregar o editar dispositivos en un grupo estático secundario

Mediante el uso de grupos secundarios estáticos, es posible clasificar los servidores según su uso, configuración, departamento de uso, clientes, etc. Puede agregar o quitar dispositivos en los grupos secundarios y, a continuación, editar, quitar, eliminar y clonar esos grupos.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. Haga clic con el botón derecho del mouse en el grupo secundario estático y, a continuación, haga clic en **Agregar dispositivos**. Para obtener información acerca de los grupos estáticos, consulte Organizar los dispositivos en grupos.
2. En el cuadro de diálogo Asistente para agregar dispositivos al nuevo grupo, seleccione las casillas de verificación de los dispositivos que se deben agregar al grupo. Los dispositivos seleccionados se indican bajo la pestaña **Todos los dispositivos seleccionados**.
3. Haga clic en **Finalizar**.
   Los dispositivos se agregan al grupo secundario estático seleccionado y aparecen en el panel derecho.

Para editar las propiedades del grupo secundario estático o para quitar dispositivos del grupo secundario estático:

1. Haga clic con el botón derecho del mouse en el grupo estático y, a continuación, haga clic en **Editar**.
2. En el cuadro de diálogo **Editar dispositivos del grupo <nombre>**, edite las propiedades del grupo y, a continuación, haga clic en **Siguiente**.
3. En el cuadro de diálogo **Selección de miembro del grupo**, seleccione o deseleccione las casillas de verificación de los dispositivos que se deben agregar o eliminar del grupo. Los dispositivos seleccionados se indican bajo la pestaña **Todos los dispositivos seleccionados**.
4. Haga clic en **Finalizar**. Los dispositivos se agregan o se quitan del grupo secundario estático seleccionado.

NOTA: Este procedimiento se aplica solo para modificar las propiedades del dispositivo de un grupo. Para quitar un dispositivo de OpenManage Enterprise o para excluir un dispositivo a nivel global, consulte Eliminar dispositivos de OpenManage Enterprise y Dispositivos de exclusión global.

Cambiar el nombre de los grupos secundarios que pertenecen a grupos estáticos o dinámicos de consulta

1. Haga clic con el botón derecho del ratón en el grupo estático o de consulta y, a continuación, haga clic en **Cambiar nombre**.

Para conocer las definiciones de grupo estático o de consulta (dinámico), consulte Organizar los dispositivos en grupos.

2. En el cuadro de diálogo **Cambiar nombre del grupo**, ingrese un nuevo nombre de grupo y haga clic en **Finalizar**.
   El nombre actualizado aparece en el panel izquierdo.

Clonar un grupo estático o de consulta

Mediante el uso de grupos estáticos o de consulta, es posible clasificar los servidores según su uso, configuración, departamento de uso, clientes, etc. Puede agregar dispositivos a los grupos estáticos o de consulta y, a continuación, editar, quitar, eliminar y clonar esos grupos. Para clonar un grupo estático o de consulta:

1. Haga clic con el botón derecho del ratón en el grupo estático o de consulta y, a continuación, haga clic en **Clonar**.
2. En el cuadro de diálogo **Clonar grupo**, ingrese el nombre y la descripción del grupo y luego seleccione un grupo principal en el cual se creará el grupo estático o de consulta clonado.
3. Haga clic en **Finalizar**.
   El grupo clonado se crea y se coloca en el grupo principal del panel de la izquierda.

   NOTA: Puede clonar solo los grupos personalizados. Debe tener los permisos "editar" y "ver". Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

   NOTA: Puede agregar dispositivos directamente bajo los grupos estáticos o de consulta clonados.

Agregar dispositivos a un grupo nuevo

1. En el panel de trabajo, seleccione la casilla de verificación correspondiente a los dispositivos, haga clic en **Agregar al grupo** y, a continuación, haga clic en **Agregar a un nuevo grupo**.
   a. En el cuadro de diálogo **Asistente para agregar dispositivos a un nuevo grupo**, escriba o seleccione los datos. 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 5.
2. 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**. Consulte Lista de dispositivos.
3. Haga clic en **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

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. En el menú **OpenManage Enterprise**, en **Dispositivos**, haga clic en **Todos los dispositivos**.
2. 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 Visualización y configuración de dispositivos.
3. En el panel de trabajo, seleccione la casilla de verificación correspondiente a los dispositivos, haga clic en **Agregar al grupo** y, a continuación, haga clic en **Agregar a grupo existente**.
   a. En el cuadro de diálogo **Agregar dispositivos a un grupo existente**, ingrese o seleccione los datos. 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 5.
4. 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**. Consulte Lista de dispositivos.
5. Haga clic en **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.

Eliminar dispositivos de OpenManage Enterprise

1. En el panel izquierdo, seleccione los dispositivos.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos, y, a continuación, haga clic en **Eliminar**.
3. Cuando se le solicite que indique si el dispositivo se excluirá globalmente, haga clic en **SÍ**.
   El dispositivo se elimina y OpenManage Enterprise deja de supervisarlo.

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 de captura en un dispositivo remoto que fue eliminado, puede quitar OpenManage Enterprise del dispositivo remoto.

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.

Información relacionada

Organizar los dispositivos en grupos

Excluir dispositivos de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Los dispositivos se agrupan según su manejo eficiente de tareas repetidas como la actualización de firmware, la detección y la generación de inventario. Sin embargo, puede excluir un dispositivo, de modo que este no forme parte de estas actividades, ya que OpenManage Enterprise no lo supervisa. Esta tarea es similar a la exclusión global. Consulte Dispositivos excluidos globalmente de los resultados de detección.

1. En el panel izquierdo, seleccione el grupo del sistema o el grupo personalizado cuyo dispositivo se debe excluir.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos y, a continuación, haga clic en **Excluir**.
3. Cuando se le pregunte si desea excluir o no los dispositivos seleccionados, haga clic en **SÍ**.
   Los dispositivos se excluyen, se agregan a la lista de exclusión global y OpenManage Enterprise deja de supervisarlos.
4. Para quitar la exclusión global y hacer que OpenManage Enterprise vuelva a supervisar el dispositivo, elimínelo del rango de exclusión global y, a continuación, vuelva a detectarlo.

Actualizar o cambiar a una versión anterior del firmware de dispositivos mediante la línea base de firmware

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Puede actualizar o degradar la versión de firmware de uno o más dispositivos:

- Página de todos los dispositivos: se recomienda para la actualización del firmware de varios dispositivos. En el menú **Dispositivos**, seleccione **Dispositivos**. Seleccione los dispositivos, haga clic en **Más accionesActualizar firmware**.
- Página de todos los dispositivos: se recomienda para la actualización del firmware de un dispositivo. En el menú **Dispositivos**, seleccione **Dispositivos**. Seleccione el dispositivo, haga clic en **Ver detallesFirmware**.
- En la página Configuración-Firmware: en el menú **Configuración**, seleccione **Firmware**. Seleccione los dispositivos, haga clic en **Comprobar el cumplimiento normativoVer informe**.

NOTA: Cuando un dispositivo está conectado, la versión de firmware no se actualiza automáticamente si es anterior a la versión de la línea base. 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 el panel izquierdo, seleccione el grupo al cual pertenecen los dispositivos. Los dispositivos asociados con el grupo se indican en la lista. Consulte Lista de dispositivos.

   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 la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos.
3. Haga clic en **Más accionesActualizar firmware**.
4. En el cuadro de diálogo **Actualizar firmware**:
   a. En la sección **Seleccionar origen**:
      - En el menú desplegable **Línea base**, seleccione la línea base que se debe utilizar para comparar y actualizar o revertir el firmware del dispositivo. Aparece una lista de dispositivos relacionados con la línea base de firmware seleccionada. El nivel de cumplimiento de cada dispositivo se muestra en la columna CUMPLIMIENTO. En función del nivel de cumplimiento, puede actualizar o degradar la versión de firmware. Para obtener más información sobre la descripción del campo en esta página, consulte Visualización del informe de cumplimiento del firmware del dispositivo. Sin embargo, cuando consulta el cumplimiento de un dispositivo individual en la página Ver detalles, puede actualizar o revertir la versión de firmware. Consulte Reversar la versión de firmware de un dispositivo individual.
        1. Seleccione las casillas de verificación correspondientes a los dispositivos que se deben actualizar.
        2. Haga clic en **Siguiente**.
      - También puede actualizar o degradar la versión mediante la utilización de un paquete de actualización individual. Haga clic en **Paquete individual** y, a continuación, siga las instrucciones que aparecen en la pantalla. Haga clic en **Siguiente**.
   b. En la sección **Requisitos previos**, aparecen los requisitos previos para el dispositivo, si los hay. Haga clic en **Siguiente**.
   c. En la sección **Programa**, seleccione:
      - **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. Puede ejecutar el trabajo más adelante.
5. Haga clic en **Finalizar**. Un trabajo de actualización de firmware se crea y aparece en la lista de trabajos. Consulte Utilización de trabajos para el control de dispositivos.

NOTA: 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.

NOTA: Si selecciona varios dispositivos, solo los dispositivos asociados con la línea base seleccionada se muestran en la tabla.

Seleccionar fuente del firmware

En la ficha **Seleccionar fuente del firmware**, puede seleccionar la línea de base o la actualización individual necesaria para actualizar el firmware.

Línea de base	Seleccione esta opción para actualizar la versión de la línea de base del firmware que desea actualizar. Seleccione la versión de la línea de base necesaria en el menú desplegable.
CUMPLIMIENTO	Indica la importancia de la actualización de firmware según el estado de cumplimiento del componente específico. Las opciones posibles son: • Correcto: la versión actual del firmware instalada en el dispositivo o componente coincide con la línea base que se define en el archivo de catálogo. • Crítico: la versión actual del firmware instalada en el componente o dispositivo es anterior a la de línea base que se define en el archivo de catálogo. Realizar la actualización es fundamental para que el dispositivo o componente funcione de manera adecuada. • Cambio a una versión anterior: la versión actual del firmware del componente o dispositivo es más reciente que el valor de referencia que se define en el archivo de catálogo. • Aviso: La versión actual del firmware instalada en el componente o dispositivo es anterior a la de línea base que se define en el archivo de catálogo. Esta actualización es una mejora para el dispositivo o componente.
MODELO	Muestra el modelo del dispositivo.
ETIQUETA DE SERVICIO	Muestra la etiqueta de servicio del dispositivo donde se actualiza el firmware.
NOMBRE/ COMPONENTES DEL DISPOSITIVO	Muestra el nombre del dispositivo o componente.

REINICIO REQUERIDO	Indica si el sistema debe reiniciarse después de instalar el firmware.
REQUISITOS PREVIOS	Muestra los requisitos previos para la actualización del firmware.
EVALUACIÓN DE IMPACTO	Muestra un mensaje sobre el impacto de la actualización del firmware.
VERSIÓN ACTUAL	Muestra la versión del firmware instalada.
VERSIÓN DE LÍNEA DE BASE	Muestra la línea de base del firmware almacenado en la línea de base.
Paquete individual	Seleccione esta opción para actualizar el firmware desde el catálogo. Haga clic en **Examinar** para navegar a la ubicación en la que se encuentra el archivo de catálogo.

Acciones

Siguiente	Muestra la ficha **Programar**.
Cancelar	Cierra el asistente sin guardar los cambios.

Reversar la versión de 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 Visualización y configuración de dispositivos. 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: Solo el firmware que se actualiza mediante la función de actualización del dispositivo individual puede revertirse.

NOTA: Si alguno de los iDRAC instalados no está en 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.

Todo firmware de dispositivo actualizado mediante el uso de la interfaz gráfica de usuario (GUI) del iDRAC no aparece aquí en la lista y no puede actualizarse. Para obtener información acerca de la creación de la línea base, consulte Crear de una línea base de firmware.

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**.
3. En el menú desplegable **Línea base**, seleccione la línea base a la que pertenece el dispositivo.
   Se enumeran 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 del firmware del dispositivo.
4. Seleccione la casilla de verificación correspondiente al dispositivo cuya versión del firmware debe revertirse, identificado por .
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).

Actualizar el inventario de dispositivos

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 recopilar el informe del inventario de un dispositivo o grupo en cualquier momento:

1. En el panel izquierdo, seleccione el grupo al que pertenece el dispositivo. Los dispositivos asociados al grupo se muestran en la lista Dispositivos.
2. Seleccione la casilla de verificación correspondiente al dispositivo y, a continuación, haga clic en **Actualizar inventario**. El trabajo se crea y aparece en la lista Trabajos, además, se identifica como **Nuevo** en la columna ESTADO DEL TRABAJO.
   De este modo, el inventario de los dispositivos seleccionados se recopila y almacena para un futuro análisis y recuperación. Para obtener más información sobre cómo ver los datos de inventario actualizados, consulte Visualización y configuración de dispositivos. Para descargar un inventario del dispositivo, consulte Exportar el inventario de un solo dispositivo.

Información relacionada

Organizar los dispositivos en grupos

Actualizar el estado del dispositivo

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 al dispositivo y, a continuación, haga clic en **Actualizar estado**.
   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.

Información relacionada

Organizar los dispositivos en grupos

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.

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 Administración de dispositivos.

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 (correcto, crítico, advertencia) se identifican mediante los respectivos símbolos de colores. Consulte Estados de los dispositivos.
- **El estado de alimentación** indica si el dispositivo está encendido o apagado.
- **El estado de la conexión** indica si un dispositivo está conectado o no a OpenManage Enterprise.
- **Nombre** indica el nombre del dispositivo.

- **El TIPO** indica el tipo de dispositivo, servidor, chasis, Dell Storage y conmutador de red.
- **La dirección IP** indica la dirección IP del iDRAC instalado en el dispositivo.
- La columna **ESTADO DE INCORPORACIÓN** indica si el dispositivo está o no incorporado. Consulte Incorporación de dispositivos.

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 Visualización y configuración de dispositivos.

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.

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.
- **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.
- **Actualizar firmware**: consulte Actualizar o cambiar a una versión anterior del firmware de dispositivos mediante la línea base de firmware.
- **Incorporación**: consulte Incorporación de dispositivos.
- **Exportar todo y seleccionados exportados**: Consulte Exportar todos los datos o aquellos seleccionados.

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.
- **Miembros apilados**

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, PDF y MS-Excel.

NOTA: No obstante, un inventario de dispositivo único solo se puede exportar a un formato .csv. Consulte Exportar el inventario de un solo dispositivo.

NOTA: 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.

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.

Visualización y configuración de dispositivos

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.

Si hace clic en **OpenManage Enterprise** > **Dispositivos** > **Todos los dispositivos** > **Seleccionar un dispositivo de la lista de dispositivos** > **Ver detalles**, puede:

- 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 EnterpriseSupervisiónInformes**.
- 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 del dispositivo.
- 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.
- 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.

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. Haga clic en la dirección IP de administración para abrir la página de inicio de sesión de iDRAC.
  - **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.
  - **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: 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.
  - Restablezca el iDRAC.
  - Extraiga y descargue el informe de SupportAssist. Consulte Extraer y descargar informes de SupportAssist.
- 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.
- 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.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage EnterpriseSupervisiónInformesInforme de la descripción general de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

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 EnterpriseSupervisiónInformesCumplimiento de firmware por informe de componentes**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

- **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 EnterpriseSupervisiónInformesInforme del disco físico**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.
- **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 EnterpriseSupervisiónInformesInforme de FRU**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.
- **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

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 la lista de trabajos. 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 problemasDescargar 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

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 la lista de trabajos. 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 14G, chasis MX7000 y sleds.

- 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 Administrar registros de auditoría.
- 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 **ExportarExportar seleccionado**.
- Para exportar todos los registros en una página, haga clic en **ExportarExportar Página actual**.

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

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. 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 -U root -P calvin <command>`
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 la lista de trabajos.
5. Haga clic en **Finalizar**.
   La sección **Alertas recientes** muestra el estado de finalización del trabajo.

   NOTA: No ejecute los siguientes comandos de RACADM:

   - `chassislog view -n all`
   - `chassislog view -n`
   - `getraclog`

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 Lista de dispositivos.

Iniciar la consola virtual

El vínculo **Consola virtual** funciona en la licencia de iDRAC Enterprise de los servidores 14G. En los servidores 12G y 13G, el vínculo funciona en las versiones 2.52.52.52 y posteriores de la licencia de OME Enterprise. Si se hace clic en el vínculo cuando la versión actual del complemento de la consola virtual es Active X, aparecerá un mensaje de petición que indica que actualice la consola para HTML 5 para mejorar la experiencia de usuario. Consulte Cambiar el tipo de complemento de consola virtual.

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.

8

Administrar el firmware del dispositivo

Si hace clic en **OpenManage EnterpriseConfiguración** y selecciona:

- **Firmware**: administra el firmware de los dispositivos mediante las líneas base de firmware.
- **Plantillas**: crea plantillas para definir la línea base de cumplimiento de la configuración y administra dichas plantillas.
- **Cumplimiento**: crea una línea base de cumplimiento de configuración del dispositivo o de un grupo de dispositivos y administra la configuración del dispositivo. Para obtener una descripción general rápida de las líneas base que se derivan de las plantillas a las que están asociadas, consulte Administrar líneas base de cumplimiento de los dispositivos a través del tablero de OpenManage Enterprise.

NOTA: Cuando un dispositivo está conectado, la versión de firmware no se actualiza automáticamente si es anterior a la versión de la línea base. 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.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol. Para administrar estas configuraciones, debe contar con credenciales de nivel de administrador de OpenManage Enterprise.

- Con la característica Firmware, puede:
  - Crear un catálogo de firmware mediante los catálogos disponibles en Dell.com o en la ruta de acceso de red. ConsulteCrear un catálogo de firmware con Dell.com o Creación de un catálogo de firmware mediante una red local. Los catálogos de firmware personalizados se utilizan para crear líneas base de firmware que sirvan como prueba local para comparar rápidamente la versión de firmware en los dispositivos con la versión en el catálogo.
  - Crear una línea base de firmware mediante los catálogos de firmware disponibles. Consulte Creación de la línea base de firmware. También puede ver el informe de línea base del firmware en el panel. Consulte Administrar las líneas base del firmware utilizando el tablero de OpenManage Enterprise.
  - Ejecutar un informe de cumplimiento para comprobar si los dispositivos relacionados con la línea base de firmware cumplen con las versiones de línea base. Consulte Comprobación de cumplimiento del firmware. La columna **CUMPLIMIENTO** muestra:
    - **Correcto** : si la versión de los dispositivos de destino es la misma que la de la línea de base del firmware.
    - **Actualización**: si los dispositivos de destino tienen una o varias versiones anteriores a la línea de base del firmware. Consulte Actualización de la versión de firmware del dispositivo.
      - Crítico Si el firmware de los dispositivos no está en cumplimiento con la línea de base del firmware. Indica que es una actualización crítica y el firmware de los dispositivos debe actualizarse para garantizar un correcto funcionamiento.
      - Advertencia Si el firmware de los dispositivos no está en cumplimiento con la línea de base del firmware y el firmware de los dispositivos puede actualizarse para mejorar su funcionamiento.
    - **Cambio a una versión anterior** Si el firmware del dispositivo es posterior a la versión de la línea de base.
  - Exportar el informe de cumplimiento para fines estadísticos y de análisis.
  - Actualice la versión de firmware del dispositivo mediante la línea base de firmware. Consulte Actualizar o cambiar a una versión anterior del firmware de dispositivos mediante la línea base de firmware.

NOTA: El nivel de cumplimiento de los dispositivos en todas las líneas base disponibles 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 varios dispositivos es Correcto y Degradar, pero si el cumplimiento de un dispositivo en el grupo es Actualizar, el nivel de cumplimiento de la línea base se indica como Actualizar.

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 Visualización y configuración de dispositivos.

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. Un gráfico de anillo y una lista de elementos en la línea base cambian en función de la línea base seleccionada en la lista de línea base. Consulte Gráfico de anillo.

Tareas relacionadas

Eliminar una línea base de firmware

Temas:

Administrar los catálogos de firmware

Los catálogos son paquetes de firmware en función de los tipos de dispositivos. En Dell.com se encuentran validados y publicados todos los catálogos disponibles (paquetes actualizados). Puede crear líneas base de firmware que descargan estos catálogos y actúan como un repositorio local de sus dispositivos. Esta práctica reduce el esfuerzo adicional que hacen los administradores y los administradores de dispositivos para acceder frecuentemente a Dell.com y también reduce en general el tiempo que demoran las actualizaciones y el mantenimiento. Para obtener información sobre definiciones de campos en la página Catálogo de administración, consulte Definiciones de campos de administración de catálogos. Los orígenes de catálogo a los que puede acceder en la actualidad son los siguientes:

- **Las versiones de firmware más recientes para los componentes en Dell.com**: Muestra las versiones de firmware más recientes 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**: es la ubicación que Dell Repository Manager (DRM) utiliza para descargar los catálogos de firmware 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.

Crear un catálogo de firmware con Dell.com

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. En la página **Administración de catálogos**, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar catálogo de firmware**:
   a) Ingrese el nombre para el catálogo de firmware y, a continuación, seleccione **Versiones más recientes de firmware de componentes en Dell.com**.
   b) Haga clic en **Finalizar**.

   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 **Firmware**, haga clic en **Volver a firmware**.

Crear un catálogo de firmware mediante una red local

1. En la página **Administración de catálogos**, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar catálogo de firmware**:
   a) Ingrese un nombre para el catálogo de firmware y, a continuación, seleccione **Ruta de red**.
   Aparece el menú desplegable **Tipo de recurso compartido**.
   b) Seleccione una de las siguientes opciones:

   NOTA: En los servidores PowerEdge 12G y 13G que tengan las versiones de iDRAC 2.52.52.52 y anteriores (solo hasta 2.50.50.50), se debe activar SMBv1 para que las características de configuración e implementación de servidor puedan funcionar.

   - NFS

1. 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.
2. 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`
3. Haga clic en **Finalizar**.

- CIFS
  1. 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.
  2. 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`
  3. En la casilla **Dominio**, ingrese el nombre de dominio del dispositivo.
  4. En la casilla **Nombre de usuario**, ingrese el nombre de usuario del dispositivo en el que se almacena el catálogo.
  5. 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
  1. 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.
  2. 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
  1. 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.
  2. 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`.
  3. En la casilla **Nombre de usuario**, ingrese el nombre de usuario del dispositivo en el que se almacena el catálogo.
  4. En la casilla **Contraseña**, ingrese la contraseña del dispositivo en el que se almacena el catálogo.
  5. 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**.

3. Haga clic en **Agregar**.
   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 **Firmware**, haga clic en **Volver a firmware**.

Tareas relacionadas

Eliminar un catálogo de firmware

Información del certificado SSL

Los archivos de catálogo para actualizaciones de firmware se pueden descargar en el sitio de asistencia 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.

Editar un catálogo de firmware

1. En la página **Administración de catálogos**, seleccione la casilla de verificación correspondiente al catálogo.
   Los detalles del catálogo de firmware se muestran en el panel derecho **<nombre del catálogo>**.
2. Haga clic en **Editar** en el panel derecho.
3. En el cuadro de diálogo **Editar catálogo de firmware**, edite las propiedades.
   Las propiedades que no puede editar aparecen atenuadas. Para obtener información sobre definiciones de campos, consulte Crear un catálogo de firmware con Dell.com y Crear un catálogo de firmware mediante una red local.
4. 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 de firmware

1. En la página **Administración de catálogos**, seleccione la casilla de verificación correspondiente al catálogo y, a continuación, haga clic en **Eliminar**.
   De este modo, se elimina de la lista el archivo de catálogo.
2. Para volver a la página **Firmware**, haga clic en **Volver a firmware**.

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

Información relacionada

Crear un catálogo de firmware mediante una red local

Crear de una línea base de firmware

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: Cuando un dispositivo está conectado, la versión de firmware no se actualiza automáticamente si es anterior a la versión de la línea base. 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.

La línea base es un conjunto de versiones de firmware personalizadas y almacenadas localmente que son de fácil acceso y aplicación. Una línea base se puede aplicar en función de una línea base a varios dispositivos, varias líneas base a un dispositivo y varias líneas base a varios dispositivos. Por ejemplo, la línea base que crea para una versión de BIOS se puede aplicar a varios servidores que ejecutan el mismo BIOS. De forma similar, se pueden aplicar dos líneas base a un dispositivo, es decir, una para la versión de firmware y la otra para el BIOS. Para crear una línea base de firmware, realice lo siguiente:

1. En **Firmware**, haga clic en **Crear línea base**.
2. En el cuadro de diálogo **Crear línea base de firmware**:
   a) En la sección **Información de línea base**:
      1. En el menú desplegable **Catálogo**, seleccione un catálogo.
      2. Para agregar un catálogo a esta lista, haga clic en **Agregar**. Consulte Administración de los catálogos de firmware.
      3. En la casilla **Nombre de línea base**, ingrese un nombre para la línea base y, a continuación, ingrese una descripción de la línea base.
      4. Haga clic en **Siguiente**.
   b) En la sección **Seleccionar dispositivos**:
      - Para seleccionar uno o más dispositivos de destino:
        1. Seleccione **Seleccionar dispositivos**, y, a continuación, haga clic en el botón **Seleccionar dispositivos**.
        2. 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.
        3. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
        4. 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:

1. Seleccione **Seleccionar grupos**, y, a continuación, haga clic en el botón **Seleccionar grupos**.
2. 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.
3. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
4. Seleccione la casilla de verificación correspondiente a los grupos. Los grupos seleccionados se indican bajo la pestaña **Grupos seleccionados**.

3. Haga clic en **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.

Eliminar una línea base de firmware

En **Firmware**, aparece una lista de las líneas base de firmware disponibles. Seleccione la casilla de verificación correspondiente a la línea base y haga clic en **Eliminar**. De este modo, se elimina la línea base de firmware y se quita de la lista de líneas base.

Comprobar el cumplimiento del firmware de un dispositivo en comparación con su línea base

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: Cuando un dispositivo está conectado, la versión de firmware no se actualiza automáticamente si es anterior a la versión de la línea base. 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.

NOTA: También puede ver el informe de línea base del firmware en el panel. Consulte Administrar las líneas base del firmware utilizando el tablero de OpenManage Enterprise.

Después de crear una línea base de firmware, puede comprobar periódicamente el cumplimiento de la versión de firmware de los componentes de un dispositivo en comparación con la versión de línea base definida mediante la utilización de un catálogo. Para comprobar el cumplimiento de la versión de firmware de un dispositivo:

1. Seleccione la casilla de verificación correspondiente a la línea base y haga clic en **Comprobar el cumplimiento normativo**.
   Se vuelve a ejecutar el trabajo de cumplimiento de línea base del firmware.

   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.

   NOTA: Al comprobar el nivel de cumplimiento de la línea base del firmware del chasis Dell EMC M1000e y VRTX, el nivel de cumplimiento se indica como 'Degradar' incluso cuando las versiones de firmware son las mismas. Esto se debe a la diferencia en la convención de nomenclatura en las versiones de firmware entre OpenManage Enterprise y FTP. Se recomienda para omitir esa condición y no degradar la versión de firmware.

2. Para ver el informe de cumplimiento y actualizar o degradar la versión de firmware de los dispositivos, haga clic en **Ver informe** en el panel derecho.

   Consulte Visualización del informe de cumplimiento del firmware del dispositivo.

Ver el informe de cumplimiento del firmware del dispositivo

El nivel de cumplimiento de los dispositivos en todas las líneas base disponibles se indica en un gráfico de anillo en la página Firmware. 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 varios dispositivos es Correcto y Degradar , pero si el cumplimiento de un dispositivo en el grupo es Crítico el nivel de cumplimiento de la línea base se indica como crítico.

Sin embargo, puede ver el cumplimiento del firmware de los dispositivos individuales relacionados con una línea base de firmware para actualizar o degradar la versión de firmware en ese dispositivo. Para ver el informe de cumplimiento del firmware del dispositivo:

- 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.

  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 del dispositivo, consulte Administrar el firmware del dispositivo.

  NOTA: Al comprobar el nivel de cumplimiento de la línea base del firmware del chasis Dell EMC M1000e y VRTX, el nivel de cumplimiento se indica como 'Degradar' incluso cuando las versiones de firmware son las mismas. Esto se debe a la diferencia en la convención de nomenclatura en las versiones de firmware entre OpenManage Enterprise y FTP. Se recomienda para omitir esa condición y no degradar la versión de firmware.
- **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 **>**.

     Aparecen una lista de componentes y su cumplimiento con respecto a la línea base de firmware.
  2. Seleccione las casillas de verificación correspondientes a los dispositivos cuyo estado de cumplimiento del firmware es Crítico y requiere una actualización.
  3. Haga clic en **Actualizar firmware**. Consulte Actualización de la versión de firmware del dispositivo.
- **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 Visualización y configuración de dispositivos.
- **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 asistencia desde donde se puede actualizar el firmware. 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 LÍNEA BASE**: indica la versión correspondiente del dispositivo disponible en la línea base de firmware.
- 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 interfaz gráfica de usuario de OpenManage Enterprise.

Actualizar la versión de firmware del dispositivo usando el informe de cumplimiento de la línea base

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: Cuando un dispositivo está conectado, la versión de firmware no se actualiza automáticamente si es anterior a la versión de la línea base. 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.

Después de ejecutar un informe de cumplimiento del firmware, si la versión de firmware en el dispositivo es anterior a la versión en el catálogo, la página Informe de cumplimiento muestra que el estado del firmware del dispositivo es Actualizar (o). Para actualizar el firmware de un dispositivo usando el informe de cumplimiento de la línea base, realice lo siguiente:

1. Seleccione la casilla de verificación correspondiente a la línea base a la que el dispositivo está conectado y, a continuación, 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. Para obtener descripciones de campos, consulte Visualización del informe de cumplimiento del firmware del dispositivo.
2. Seleccione la casilla de verificación correspondiente al dispositivo cuyo firmware se debe actualizar. Puede seleccionar más de un dispositivo con propiedades similares.
3. Haga clic en **Actualizar firmware**.
4. En el cuadro de diálogo **Actualizar firmware**, seleccione:
   - **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. Este modo se recomienda si no desea alterar sus tareas actuales.
5. Haga clic en **Actualizar**.

   NOTA: Para actualizar un dispositivo, debe asociar el dispositivo y el catálogo entre sí.

Editar la línea base de firmware

1. Seleccione la casilla de verificación correspondiente a la línea 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 **Firmware**, haga clic en **Volver a firmware**.

Eliminar una línea base de firmware

Seleccione la casilla de verificación correspondiente a la línea base y haga clic en **Eliminar**. De este modo, se elimina la línea base de firmware y la información actualizada se muestra en la lista Línea base.

Información relacionada

Administrar el firmware del dispositivo

9

Administrar las plantillas de configuración de dispositivos

En el menú **OpenManage Enterprise**, si hace clic en **Configuración** > **Implementar**, puede establecer las propiedades de configuración, como las propiedades de red, las versiones de BIOS de los servidores y el chasis, mediante las plantillas de configuración de dispositivos, las cuales pueden ser predefinidas o personalizadas. Las plantillas permiten optimizar los recursos del centro de datos y la amplitud de banda de los expertos en la materia (PYME), además de reducir el tiempo de ciclo en la creación de clones e implementaciones. Las plantillas mejoran sus operaciones de negocios críticas en infraestructura convergente que utilizan infraestructuras definidas por software.

Temas:

Crear una plantilla desde un dispositivo de referencia

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: En los servidores PowerEdge 12G y 13G que tengan las versiones de iDRAC 2.52.52.52 y anteriores (solo hasta 2.50.50.50), se debe activar SMBv1 para que las características de configuración e implementación de servidor puedan funcionar.

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

1. En el menú **OpenManage Enterprise**, haga clic en **Configuración** > **Implementar** > **Crear plantillas** 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 configuración del dispositivo.
   b) Seleccione el tipo de plantilla:
      - **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.
   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 la creación de la plantilla nueva. 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.

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 utilizando un servidor como dispositivo, puede seleccionar clonar las propiedades del servidor, como iDRAC, BIOS, Lifecycle Controller y los filtros de eventos. Por ejemplo, iDRAC y RAID. 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 y el estado se muestra en la columna **ESTADO**.

La información del trabajo también se muestra en la página **Supervisión** > **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 importando un archivo de plantilla

NOTA: En los servidores PowerEdge 12G y 13G que tengan las versiones de iDRAC 2.52.52.52 y anteriores (solo hasta 2.50.50.50), se debe activar SMBv1 para que las características de configuración e implementación de servidor puedan funcionar.

1. En el menú **OpenManage Enterprise**, haga clic en **Configuración** > **Implementar** > **Crear plantilla** y luego seleccione **Importar desde archivo**.
2. En el cuadro de diálogo **Importar plantilla**:
   a) Introduzca un nombre para la nueva plantilla.
   b) Haga clic en **Seleccionar un archivo** y, a continuación, seleccione un archivo de plantilla.
   c) Seleccione **Servidor** o **Chasis** 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 nueva.

- Para ver la información de una plantilla, 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. Consulte Implementar las plantillas de dispositivos y Crear una plantilla desde un dispositivo de referencia.
- Para editar una plantilla realice lo siguiente:
  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 y, a continuación, haga clic en **Finalizar**. La información actualizada se muestra en la lista de plantillas.

Ver la información de una plantilla

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

1. En la lista de plantillas, 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, su descripción, el dispositivo de referencia del cual se creó la plantilla de configuración 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. 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 plantilla

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

- La vista guiada le permite editar los atributos, como el BIOS, la secuencia de arranque y las redes. Si los elementos de configuración no se establecieron durante la creación de la plantilla, no se mostrarán durante el modo de edición.
- El modo Avanzado le permite editar todos los valores disponibles de configuración del servidor.

1. Seleccione la casilla de verificación de la plantilla personalizada requerida 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. No se puede editar el tipo de plantilla.
   b) Haga clic en **Siguiente**.
   c) En la sección **Editar Componentes**, los atributos de la plantilla se muestran en:
      - Vista guiada: muestra el BIOS, el arranque y la configuración de red de la plantilla seleccionada.
      - Vista avanzada: muestra todas las propiedades de la plantilla seleccionada.

      1. 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.
      2. 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.
      3. Haga clic en **Redes**. Todas las redes asociadas con la plantilla se muestran en las **Interfaces de red**.
         - Para asociar un grupo de identidad opcional con la plantilla, seleccione en el menú desplegable el **grupo de identidad**. Se muestran las redes asociadas con el grupo de identidad seleccionado. Si la plantilla se edita en la vista Avanzada, se desactiva la selección del grupo de identidad para esta plantilla.
           - 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 (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.
3. Haga clic en **Siguiente**.
   En la sección **Resumen**, se muestran los atributos que editó utilizando el modo 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.

Editar las propiedades de red

Puede editar la configuración de red de cualquier plantilla que contenga atributos aplicables de NIC. Los campos del número de serie de NIC, del identificador de NIC, del número de puerto y de la partición son de solo lectura.

1. Edite las siguientes opciones, según corresponda:
   - **Ancho de banda mínimo (%)**: ancho de banda mínimo de la partición.
   - **Ancho de banda máximo (%)**: ancho de banda máximo de la partición.
   - **Red sin etiqueta** y **Red con etiqueta**: corresponde solo para las plantillas creadas mediante los servidores modulares, seleccione redes con etiqueta y sin etiqueta.

2. Haga clic en **Finalizar**.

Se guardan las propiedades actualizadas de la red.

Implementar las plantillas de dispositivos

Puede implementar una plantilla que incluye un conjunto de atributos de configuración para dispositivos específicos. La implementación de una plantilla de configuración de dispositivos en los dispositivos asegura que los dispositivos estén configurados de manera uniforme.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 ejemplo. Consulte Crear una plantilla desde un dispositivo de referencia.
- Los dispositivos de destino cumplen con los requisitos especificados en Requisitos mínimos del sistema para implementar OpenManage Enterprise.
- La licencia de administración de configuración de servidor de OpenManage se instala en los dispositivos de destino.

PRECAUCIÓN: Asegúrese de que se seleccionen solo los dispositivos apropiados para la implementación. Después de implementar una plantilla de configuración 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 la página **Configuración** > **Implementar**, seleccione la casilla de verificación que corresponde a la plantilla que desea implementar y luego 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 del dispositivo, es posible que cambiar la configuración requiera un reinicio forzado el 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) 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.
   c) Haga clic en **Siguiente**.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte Definiciones de los campos Programar trabajos.
5. Haga clic en **Finalizar**. Revise el mensaje de advertencia y, a continuación, haga clic en **SÍ**.
   Un trabajo de configuración de dispositivo se crea en Trabajos. Consulte Utilización de trabajos para el control de dispositivos.

Clonar plantillas

1. En el menú **OpenManage Enterprise**, en **Configuración**, haga clic en **Implementar**.
   Se puede ver una lista de plantillas 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 nueva y, a continuación, haga clic en **Finalizar**.
   La plantilla clonada se crea y se muestra en la lista de plantillas.

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.

Se sabe que no tienen estado los servidores implementados mediante una plantilla de configuración de dispositivos que contiene identidades de E/S virtuales. 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.

La pestaña **Grupos de identidades** permite crear, editar, eliminar o exportar grupos de E/S virtuales.

Descripción general de la implementación sin estado

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

1. **Cree una plantilla de dispositivo:** haga clic en la tarea **Crear plantilla**, en la pestaña **Implementar**, para crear una plantilla de dispositivo. 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 dispositivo en el panel **Plantillas** y haga clic en **Editar red** para asignar un grupo de identidades a la plantilla de dispositivos. 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 dispositivo en dispositivos de destino**: utilice la tarea **Implementar plantilla** en la pestaña **Implementar** para implementar la plantilla de dispositivos y las identidades virtuales en los dispositivos de destino.

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.

Nombre del bloque	Introduzca un nombre del grupo de identidades. El nombre del grupo puede tener una longitud máxima de 255 caracteres.
Descripción	Introduzca una descripción para el grupo de identidades. La longitud máxima de esta propiedad es 255 caracteres.

Acciones

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

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:

- Identidad Ethernet que se define por la Dirección de control de acceso al medio (MAC). Las direcciones MAC son necesarias para las comunicaciones de Ethernet (LAN).
- Fibre Channel (FC) identidad que está definida por el nombre de nodo mundial (WWNN) y 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.
- Identidad iSCSI que se define mediante el nombre calificado iSCSI (IQN). Las identidades de IQN son necesarias para admitir el inicio desde SAN por medio del protocolo iSCSI.

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

Crear grupos de identidades

Puede crear un grupo de identidades que contenga uno o varios tipos de identidades virtuales.

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.

Create Identity Pool - iSCSI

You can configure the required number of iSCSI MAC addresses in the iSCSI tab.

NOTA: The iSCSI attributes are applied only when the DHCP option for iSCSI Initiator is disabled in the source template.

Include iSCSI MAC Addresses
Select the check box to add the iSCSI MAC addresses to the identity pool.

Starting MAC Address
Enter the starting MAC address of the identity pool in one of the following formats:

- `AA:BB:CC:DD:EE:FF`
- `AA-BB-CC-DD-EE-FF`
- `AABB.CCDD.EEFF`

The maximum length of a MAC address is 50 characters. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

Number of iSCSI MAC addresses
Enter the number of iSCSI MAC addresses. The MAC address can be between 1 and 5000. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

Configure iSCSI Initiator
Select the check box to configure the iSCSI initiator. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.

IQN Prefix
Enter the IQN prefix of iSCSI identity pool. The length of the IQN prefix is a maximum of 200 characters. The system generates the pool of IQN addresses automatically by appending the generated number to the prefix. For example: `<IQN Prefix>.<number>`

This option is displayed only if the **Configure iSCSI Initiator** check box is selected.

NOTA: The IQN configured with identity pools is not deployed on the target system if the boot mode is "BIOS".

NOTA: If the iSCSI initiator name is displayed in a separate line in the Identity Pools > Usage > iSCSI IQN field, then, it indicates that the iSCSI IQN is enabled only on that NIC partition.

Enable iSCSI Initiator IP Pool	Select the check box to configure a pool of iSCSI initiator identities. This option is displayed only if the **Include iSCSI MAC Addresses** check box is selected.
IP Address Range	Enter the IP address range for the iSCSI initiator pool in one of the following formats: • `A.B.C.D - W.X.Y.Z` • `A.B.C.D/E`
Subnet mask	Select the subnet mask address of the iSCSI pool from the drop-down.
Gateway	Enter the gateway address of the iSCSI pool.
Primary DNS Server	Enter the primary DNS server address.
Secondary DNS Server	Enter the secondary DNS server address.

NOTA: The IP Address Range, Gateway, Primary DNS Server, and Secondary DNS Server must be valid IPv4 addresses.

Actions

Previous	Displays the **Ethernet** tab.
Next	Displays the **FCoE** tab.
Finish	Saves the changes and displays the Configuration page.
Cancel	Closes the **Create Identity Pool** wizard without saving the changes.

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 de inicio	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 de inicio	Ingrese la dirección MAC 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.

Definir redes

1. Seleccione **Configuración** > **Redes** > **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.
4. Haga clic en **Finalizar**.

La red configurada actualmente en su entorno ahora está definida y los recursos pueden acceder a la red. También puede exportar la lista de redes como un archivo .csv haciendo clic en el botón **Exportar**.

Tipos de red

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

Tabla 10. Tipos de red

Tipos de red	Descripción
Propósito general Bronze	Se utiliza para tráfico de datos de prioridad baja.
Propósito general Gold	Se utiliza para tráfico de datos de prioridad alta
Propósito general Silver	Se utiliza para tráfico de datos de prioridad estándar o predeterminada
Propósito general Platinum	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 de iSCSI	Se utiliza para las VLAN de iSCSI
Almacenamiento de FCoE	Se utiliza para las VLAN de FCoE
Almacenamiento de reproducción 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. En la página **Configuración**, haga clic en **Redes**.
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: Debido a que el direccionamiento IPv6 no es compatible con el agregador M de E/S (IOA) ni con los módulos FN de E/S, la configuración de VLAN en el chasis M1000e y FX2 no es compatible con una IPv6 infra.

   NOTA: En OpenManage Enterprise 3.1, 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**.

Implementación sin estado

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Antes de realizar una implementación sin estado, asegúrese de que:

- Haya creado una plantilla de implementación de dispositivos o clonado una plantilla de ejemplo. Consulte Crear una plantilla desde un dispositivo de referencia.
- Haya creado y configurado un grupo de identidades. Consulte Crear grupos de identidades.
- Los dispositivos de destino cumplen con los requisitos especificados en Requisitos mínimos del sistema para implementar OpenManage Enterprise.
- La licencia de OpenManage Enterprise está instalada en todos los dispositivos de destino.

NOTA: Los grupos de identidad no se pueden asociar a plantillas creadas en versiones anteriores de OpenManage Enterprise.

1. En la lista de plantillas, seleccione la casilla de verificación correspondiente al dispositivo cuya plantilla debe implementarse.
2. Haga clic en **Editar red**.
3. En el cuadro de diálogo **Editar red**, seleccione el grupo de identidades y la red con etiqueta y sin etiqueta.
4. Ingrese el ancho de banda máximo y mínimo y, a continuación, haga clic en **Finalizar.**
5. En la página **Detalles de la plantilla**, haga clic en **Implementar plantilla**.
6. En el cuadro de diálogo **Implementar plantilla: <nombre de la plantilla>**, en **Destino**:
   a) Haga clic en **Seleccionar** y, a continuación, seleccione dispositivos en el cuadro de diálogo **Destino del trabajo** y haga clic en **Aceptar**. Consulte Selección de dispositivos y grupos de dispositivos destino.
   b) Haga clic en **Siguiente**.
7. En la sección **Inicio para la imagen ISO de red**:
   a) Seleccione la casilla de verificación **Inicio para la imagen ISO de red**. Esta casilla de verificación aparece solo si el dispositivo objetivo es un servidor.
   b) Seleccione **CIFS** o **NFS** y, a continuación, ingrese la información en los campos como, por ejemplo, ruta de acceso del archivo de imagen .ISO y ubicación del recurso compartido en el que se almacenará el archivo de imagen .ISO.
   c) Haga clic en **Siguiente**.
8. En la sección **IP de administración de iDRAC**, cambie la configuración de IP del dispositivo de destino y haga clic en **Siguiente**.
   NOTA: 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.
9. En la sección **Configuraciones de NIC**, haga clic en **Asignar identidades**.
10. Se muestran las identidades virtuales asignadas de las tarjetas NIC. Para ver todas las identidades asignadas del grupo de identidades, haga clic en **Ver todos los detalles de NIC** y, a continuación, haga clic en **Siguiente**.
11. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos.
12. Haga clic en **Finalizar**. Revise el mensaje y, a continuación, haga clic en **SÍ**.
    Un trabajo de configuración de dispositivo se crea en Trabajos. Consulte Utilización de trabajos para el control de dispositivos.

Eliminar grupos de identidades

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

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.

Recuperación de identidades virtuales asignadas

Puede recuperar las identidades virtuales asignadas desde un dispositivo según su preferencia.

Para recuperar las identidades virtuales asignadas, realice lo siguiente:

1. En la página **Nombre de dispositivo**, dentro de la opción **Descripción general**, haga clic en **Perfil de configuración** > **Recuperar identidades**.
   Se muestra la página Recuperar identidades.
2. Si desea continuar con la recuperación de las identidades virtuales asignadas del dispositivo, haga clic en **Sí**.

   NOTA: Durante el proceso de recuperación, las identidades que no estén implementadas desde OpenManage Enterprise no se recuperan y el trabajo Configuración de sistema falla. Para recuperar estas identidades, debe utilizar la opción "Forzar recuperación de identidades si falla la eliminación".

Una vez que las identidades se recuperan, se pueden asociar con una plantilla de configuración diferente para las tareas de implementación sin estado.

Migración de perfil de dispositivo

Puede migrar los atributos de una plantilla de configuración de dispositivo y las identidades virtuales del dispositivo de origen a dispositivos de destino. Los dispositivos de destino deben tener un sistema Lifecycle Controller y valores de configuración iDRAC, BIOS, RAID, NIC para servidores, y CMC para chasis idénticos a los del dispositivo de origen.

Para migrar el perfil, realice lo siguiente:

1. En la página **Nombre de dispositivo**, dentro de la opción **Descripción general**, haga clic en **Perfil de configuraciónMigrar perfil**.
2. Seleccione el dispositivo de destino con la misma configuración de hardware que el dispositivo de origen.

   NOTA: Durante el proceso de migración, las identidades que no estén implementadas desde OpenManage Enterprise no se migran y el trabajo Configuración de sistema falla. Para migrar estas identidades, debe utilizar la opción "Forzar migración si falla la eliminación de perfil".

   PRECAUCIÓN: Cuando se utiliza la opción "Forzar migración si falla la eliminación de perfil", existe la posibilidad de que las identidades se dupliquen si el dispositivo de origen está encendido.
3. Haga clic en **Migrar perfil**.
   Las identidades virtuales ahora se recuperan desde el dispositivo de origen y se pueden asignar al dispositivo de destino.

10

Administración del cumplimiento de la configuración del dispositivo

Si selecciona **OpenManage Enterprise** > **Configuración** > **Cumplimiento**, puede crear líneas de base de configuración utilizando las plantillas de cumplimiento integradas o creadas por el usuario. Puede crear una plantilla de cumplimiento de configuración 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 Privilegios de usuario de OpenManage Enterprise basados en el rol. Consulte también Administrar líneas base de cumplimiento de los dispositivos a través del tablero de OpenManage Enterprise.

NOTA: Después de que se crea una línea base de configuración utilizando una plantilla, el resumen del nivel de cumplimiento de cada línea base se muestra en una tabla. Cada dispositivo tiene su propio estado, 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: Puede crear una línea de base de configuración solo del chasis principal MX7000.

En la página Cumplimiento, puede:

- Crear una línea base de cumplimiento de la configuración. Consulte Crear la línea base de cumplimiento de una configuración.
- Comprobar el cumplimiento de los dispositivos o grupos de dispositivos contra la línea base de cumplimiento de la configuración.
- Administrar las plantillas de cumplimiento. Consulte Administrar plantillas de línea base de cumplimiento.

Utilice los datos de la línea base de cumplimiento de configuración para establecer directivas de alerta que le notifican si una política de línea base se desvía. La alerta se genera en función de una línea base de cumplimiento que puede verse en la página del panel de OpenManage Enterprise. Para obtener más información sobre la configuración de políticas de alerta, consulte Supervisión de alertas de dispositivos.

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.

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.

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** > **Supervisión** > **Informes** > **Dispositivos por base de línea de cumplimiento de plantilla** y luego haga clic en **Ejecutar**. Consulte Ejecutar informes.

Tareas relacionadas

Crear la línea base de cumplimiento de una configuración
Editar una línea base de cumplimiento de configuración
Eliminar una línea base de cumplimiento de configuración
Administrar plantillas de línea base de cumplimiento
Seleccionar los criterios de una consulta

Temas:

- Administrar plantillas de línea base de cumplimiento
- Crear la línea base de cumplimiento de una configuración
- Editar una línea base de cumplimiento de configuración
- Corrección de dispositivos no compatibles
- Eliminar una línea base de cumplimiento de configuración

Administrar plantillas de línea base 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. Puede crear plantillas de línea base utilizando una plantilla de implementación, un dispositivo de referencia o mediante la importación desde un archivo. Consulte Administrar plantillas de línea base de cumplimiento.

Si selecciona **Configuración** > **Cumplimiento** > **Administración de plantillas**, puede ver la lista de plantillas de cumplimiento. En esta página:

- Puede crear una plantilla de cumplimiento:
  - Mediante una plantilla de implementación. Consulte Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación.
  - Mediante un dispositivo de referencia. Consulte Crear una plantilla de línea base de cumplimiento a partir de un dispositivo de referencia.
  - Mediante la importación desde un archivo de plantilla. Consulte Crear una línea base de cumplimiento mediante la importación desde un archivo.
- Editar una plantilla de cumplimiento. Consulte Editar una plantilla de cumplimiento de línea base.
- Clonar una plantilla de cumplimiento. Consulte Clonar una plantilla de línea base de cumplimiento.
- 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.
- Eliminar una plantilla de cumplimiento. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Eliminar**.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo
Editar una línea base de cumplimiento de configuración
Eliminar una línea base de cumplimiento de configuración
Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación
Editar una plantilla de cumplimiento de línea base

Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación

1. Haga clic en **ConfiguraciónCumplimientoAdministración de plantillasCrearDesde la plantilla de implementación**.
2. En el cuadro de diálogo **Clonar plantilla de implementación**, en el menú desplegable **Plantilla**, seleccione una plantilla que se debe utilizar como la línea base para la nueva plantilla.
3. Ingrese un nombre y una descripción para la plantilla de cumplimiento de línea de base.
4. Haga clic en **Finalizar**.
   Se creará una plantilla de cumplimiento y aparecerá en la lista de líneas de base de cumplimiento de la configuración.

Tareas relacionadas

Administrar plantillas de línea base de cumplimiento
Clonar una plantilla de línea base de cumplimiento

Crear una plantilla de línea base 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.

1. Haga clic en **ConfiguraciónCumplimiento Administración de plantillasCrearA partir de dispositivo de referencia**.
2. En el cuadro de diálogo **Crear plantilla de cumplimiento**, ingrese un nombre y una descripción para la plantilla de cumplimiento de línea de base.
3. Seleccione las opciones para crear la plantilla 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 dispositivo maestro para crear la plantilla. Consulte Seleccionar dispositivos y grupos de dispositivos de destino.
   a) Si selecciona "servidor" como dispositivo maestro, seleccione también 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 línea base de cumplimiento que se creó recientemente aparece en la página **Plantillas de cumplimiento**.

Crear una línea base de cumplimiento mediante la importación desde un archivo

1. Haga clic en **Configuración** > **Cumplimiento** > **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 de línea base.
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 una línea base de cumplimiento de configuración.

Clonar una plantilla de línea base de cumplimiento

1. Haga clic en **Configuración** > **Cumplimiento** > **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.
4. Haga clic en **Finalizar**.
   De este modo, se crea la nueva plantilla y se agrega a **Plantillas de cumplimiento**.

Información relacionada

Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación
Editar una plantilla de cumplimiento de línea base

Editar una plantilla de cumplimiento de línea base

Si desea editar las propiedades de la línea base de configuración, puede editar las propiedades de la plantilla vinculada a ella.

PRECAUCIÓN: Si la plantilla 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.

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.

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 **Finalizar**.
   La plantilla queda editada y la información actualizada se guarda.

Tareas relacionadas

Administrar plantillas de línea base de cumplimiento
Clonar una plantilla de línea base de cumplimiento

Crear la línea base de cumplimiento de una configuración

OpenManage Enterprise puede asignar 10 líneas base a un solo dispositivo y comprobar el nivel de cumplimiento de un máximo de 500 dispositivos a la vez. Para ver la lista de las líneas base, haga clic en **OpenManage EnterpriseConfiguraciónCumplimiento**.

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.
- El uso de una plantilla capturada de un dispositivo de soporte. Consulte Crear una plantilla de línea base de cumplimiento a partir de un dispositivo de referencia.
- El uso de una plantilla importada desde un archivo. Consulte Crear una línea base de cumplimiento mediante la importación desde un archivo.

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.

PRECAUCIÓN: Si la plantilla 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** > **Crear línea de 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.
   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.

   NOTA: Solo se muestran los dispositivos compatibles. Si selecciona un grupo, los dispositivos que no son compatibles con la plantilla de línea base 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 **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.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo

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.

PRECAUCIÓN: Si la plantilla 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 de línea base. 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**.
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.

Tareas relacionadas

Administrar plantillas de línea base de cumplimiento

Seleccionar los criterios de una consulta

Información relacionada

Administración del cumplimiento de la configuración del dispositivo

Eliminar una línea base de cumplimiento de configuración

Corrección de dispositivos no compatibles

Puede corregir los dispositivos que no se ajustan a la línea base asociada cambiando los valores de atributos para que coincidan con los atributos de la línea base asociada. Para ver los atributos cambiados, desde el informe de cumplimiento de dispositivos, haga clic en **Ver informe**. En la tabla **Informe de cumplimiento**, 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**.
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.

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.

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 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**.
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

Seleccionar los criterios de una consulta

Administrar plantillas de línea base de cumplimiento

Editar una línea base de cumplimiento de configuración

Información relacionada

Administración del cumplimiento de la configuración del dispositivo

11

Supervisión de alertas de dispositivos

Si hace clic en el menú **OpenManage Enterprise** y selecciona elementos en **Alertas**, puede:

- Supervisar alertas por:
  - Confirmar alertas
  - Ignorar alertas
  - Visualizar las alertas archivadas y Descargar las alertas archivadas
- Crear y administrar directivas de alerta. Consulte Directivas de alerta.
- Ver definiciones de alerta. Consulte Definiciones de alerta.
- Exportar todos los datos de alertas o los datos de alertas seleccionados. Consulte Exportación de datos.

  NOTA: Actualmente, OpenManage Enterprise solo recibe las alertas SNMPv1 y SNMPv2 desde los siguientes servidores PowerEdge: MX740c, MX840c y MX5016s.

NOTA: Para administrar estas configuraciones, debe contar con credenciales de nivel de administrador de OpenManage Enterprise. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 EnterpriseSupervisiónInformesCuentas de alertas por informe de dispositivos**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

Conceptos relacionados

Visualizar los registros de alertas

Tareas relacionadas

Eliminar alertas

Temas:

Visualizar los registros de alertas

Haga clic en **OpenManage Enterprise** > **Configuración** > **Alertas** > **Registro de alertas**. Se muestra una lista de alertas. En la lista aparecen la gravedad de las alertas, el tiempo en que se generó, el dispositivo de origen que generó la alerta, la categoría de alerta y el mensaje de alerta.

- GRAVEDAD: indica la gravedad de una alerta.
- RECONOCIMIENTO: muestra una marca visto cuando se visualiza y reconoce una alerta. El número total de las alertas generadas también se muestra en el encabezado de OpenManage Enterprise. Consulte Descripción general de interfaz gráfica de usuario de OpenManage Enterprise.
- Haga clic en el nombre del dispositivo de hiperenlace en **NOMBRE DE ORIGEN** para ver y configurar las propiedades del dispositivo que generó la alerta. Consulte Visualización y configuración de dispositivos.

  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: indica la categoría de la alerta. Por ejemplo, el estado del sistema y la auditoría.

  En la columna **CONFIRMAR** correspondiente a una alerta aparece una marca visto cuando se ve y se confirma la alerta.

En esta página puede confirmar, anular la confirmación, omitir, exportar, eliminar y archivar datos de alerta. Para obtener más información sobre el archivo de las alertas, consulteVisualizar las alertas archivadas.

Tareas relacionadas

Eliminar alertas

Información relacionada

Supervisión de alertas de dispositivos

Confirmar alertas

Después de ver una alerta y entender su contenido, puede confirmar que ha leído el mensaje de alerta. Para confirmar, seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **Confirmar**. Una marca visto aparece en la columna **CONFIRMAR**.

No confirmar alertas

Puede anular la confirmación de una alerta si es incorrecta o está repetida. Seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **Anular confirmación**. Se elimina la marca visto correspondiente a la alerta en la columna **CONFIRMAR**. O puede hacer clic en la marca visto para anular la confirmación de un mensaje de alerta ya confirmado.

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 **Omitir**. 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.

Eliminar alertas

Puede quitar una alerta para eliminar permanentemente la aparición de la alerta de la consola. Para evitar que la alerta vuelva a aparecer en OpenManage Enterprise, omita la alerta. Consulte Ignorar alertas.

1. 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.
2. Haga clic en **Sí**.
   De este modo, se elimina la alerta.

La cantidad total de alertas que se muestran en la fila de encabezado de OpenManage Enterprise disminuye.

Conceptos relacionados

Visualizar los registros de alertas

Información relacionada

Supervisión de alertas de dispositivos

Visualizar las alertas archivadas

Se puede generar y ver un máximo de 50.000 alertas al mismo tiempo mediante la utilización de 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 11. 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. Consulte Descargar las 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 y se almacenan en un archivo .CSV y, a continuación, 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: Nota: Para descargar alertas archivadas, debe tener los privilegios necesarios. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Directivas de alerta

Si hace clic en **OpenManage EnterpriseAlertasDirectivas de alertas**, puede:

- Desencadenar acciones automáticamente en función de la entrada de una alerta.
- Enviar las alertas a direcciones de correo electrónico, teléfono, capturas SNMP y realizar acciones de control de alimentación de los dispositivos, como encender o apagar un dispositivo cuando se genera una alerta de una categoría predefinida.
- Crear, editar, habilitar, deshabilitar y eliminar las directivas de alerta.

Una marca visto correspondiente a una directiva de alerta indica que la política está activada. Cuando se recibe una alerta que cumple con los criterios de la política, puede configurar la política para llevar a cabo acciones como el envío de un mensaje de correo electrónico y la activación del reenvío de capturas SNMP. Una vez que se realice la configuración anterior, puede hacer lo siguiente:

- Enviar un mensaje de correo electrónico:
  1. Haga clic en la celda **CORREO ELECTRÓNICO** correspondiente a la directiva de alerta.
  2. En el cuadro de diálogo **Acciones de alerta: correo electrónico**, escriba la información del mensaje que desea enviar. Utilice el modelo de mensaje indicado en los cuadros de texto.
  3. Haga clic en **Finalizar**. Se muestra una marca visto en la celda. El mensaje de correo electrónico se envía cuando se recibe una alerta que cumple con los criterios de la política definida.
- Reenviar una captura de SNMP:
  1. Haga clic en la celda **CAPTURA SNMP** correspondiente a la directiva de alerta.
  2. Cuando se le solicite, haga clic en **SÍ**.
  3. En Alertas, expanda **Configuración de SNMP**.
  4. Realice las tareas en Configurar alertas de SMTP, SNMP y Syslog. Se muestra una marca visto en la celda. Una captura SNMP se activa cuando se recibe una alerta que cumple con los criterios de la política definida.
- Ignorar la directiva de alerta:

1. Haga clic en la celda **IGNORAR** correspondiente a la directiva de alerta.
2. Cuando se le indique que todas las acciones asociadas con la política se eliminarán, haga clic en SÍ**.** Se muestra una marca visto en la celda. Cualquier alerta recibida que cumpla con los criterios de la política será ignorada.

- Enviar notificaciones a un dispositivo móvil. Debe configurar OpenManage Enterprise y el teléfono móvil para enviar notificaciones emergentes. Consulte Configuración de OpenManage Mobile.

  1. Haga clic en la celda **MÓVIL** correspondiente a la directiva de alerta. Si está activado, la política está desactivada y desaparece la marca de verificación. Viceversa si está deshabilita.

- Enviar un mensaje SMS:

  1. Haga clic en la celda **SMS** correspondiente a la directiva de alerta.
  2. En el cuadro de diálogo **Acciones de alerta: SMS**, escriba el número de teléfono.
  3. Haga clic en **Finalizar**. Se muestra una marca visto en la celda. El mensaje SMS se envía cuando se recibe una alerta que cumple con los criterios de la política definida.

     NOTA: Se envía un SMS solo a los teléfonos móviles estadounidenses.

- Realizar una acción de control de alimentación en el dispositivo:

  1. Haga clic en la celda **CONTROL DE ALIMENTACIÓN** correspondiente a la directiva de alerta.
  2. En el cuadro de diálogo **Acciones de alerta: Control de alimentación**, seleccione esta opción para indicar si desea realizar un ciclo de encendido, apagar o encender un dispositivo.
  3. Haga clic en **Finalizar**. Se muestra una marca visto en la celda. El mensaje SMS se envía cuando se recibe una alerta que cumple con los criterios de la política definida.

- Ejecutar un script remoto:

  1. Haga clic en la celda **Ejecución de script remoto** correspondiente a la directiva de alerta.

     NOTA: Debido a que la función de secuencias de comandos remotas solo es compatible en servidores Linux, los comandos SSH solo se pueden ejecutar en servidores Linux, pero no en los servidores Windows.
  2. Cuando se le solicite, haga clic en **SÍ**.
  3. En la pestaña **Ejecución de script**, en **Configuración de comandos remotos**, realice las tareas de Crear un trabajo de comando remoto para la administración de dispositivos. Se muestra una marca visto en la celda. El comando especificado se ejecuta cuando se recibe una alerta que cumple con los criterios de la política definida.

Tareas relacionadas

Eliminar políticas de alerta
Inhabilitar políticas de alerta
Habilitar políticas de alerta
Editar políticas de alerta
Crear políticas de alerta

Crear políticas de alerta

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. Haga clic en **Directivas de alertaCrear**.
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) Para habilitar una directiva de alerta de manera predeterminada, seleccione la casilla de verificación **Habilitar directiva**.
   b) Haga clic en **Siguiente**.
3. En la sección **Categoría**, seleccione la casilla de verificación **Todas** para aplicar la directiva de alerta a todas las categorías disponibles. De manera predeterminada, se muestran las siguientes categorías, pero no se aplican. Para ver las subcategorías dentro de cada categoría, expanda la categoría:
   a) Haga clic en **Siguiente**.
4. En la sección **Destino**, agregue los dispositivos o los grupos. Consulte Seleccionar dispositivos y grupos de dispositivos de destino.
   - Para especificar un dispositivo no detectado (dispositivo de terceros), seleccione **Dispositivos específicos no detectados** y, a continuación, escriba la dirección IP o el nombre de host.
   - Para especificar cualquier dispositivo no detectado, seleccione **Cualquier dispositivo no detectado**.

NOTA: No se pueden realizar las tareas Ejecución de script remoto ni Acción de encendido en los dispositivos no detectados.

NOTA: Se pueden omitir las alertas de dichos dispositivos externos y 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).

- Haga clic en **Siguiente**.

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 la alerta para la cual se debe activar esta directiva.
   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 una o varias casillas de verificación para iniciar las siguientes acciones cuando se ejecute la política:
   - Envíe un correo electrónico a un destinatario designado mediante la selección de la casilla de verificación **Correo electrónico**, y especifique los datos en los campos.
   - Configure alertas de SNMP haciendo clic en **Habilitar** junto a la casilla de verificación **Reenvío de capturas SNMP**. En el cuadro de diálogo **Configuración de SNMP**, ingrese o seleccione los datos. Consulte Configurar alertas de SMTP, SNMP y Syslog.
   - Configuración de las propiedades de Syslog.
   - Seleccione la casilla de verificación **Omitir** para omitir un mensaje de alerta y no activar la directiva de alerta.
   - Envíe un SMS a un número de teléfono; para ello, ingrese un número de teléfono en la casilla **Para**.
   - Controlar la alimentación del dispositivo mediante ciclo de apagado y encendido, encendido o apagado del dispositivo. Para apagar un OS antes de realizar las acciones de control de alimentación, seleccione la casilla de verificación **Primero apagar OS**.
   - Ejecute un comando remoto. Para ello, haga clic en **Habilitar** junto a **Ejecución de script remoto**:
     - En el cuadro de diálogo **Configuración de comandos remotos**, escriba o seleccione información para establecer los comandos remotos que desea ejecutar. Consulte Ejecutar comandos y scripts remotos.
     - En el menú desplegable, seleccione el script que desea ejecutar cuando se ejecute esta directiva de alerta. Puede configurar la ejecución del comando remoto también como se describe en Administración de los ajustes del servidor OpenManage Enterprise.
   - **Móvil**: envía notificaciones a los teléfonos móviles registrados con esta versión de OpenManage Enterprise. Consulte Configuración de OpenManage Mobile.
8. Haga clic en **Siguiente**.
9. En la sección **Resumen**, se muestran los detalles de la directiva 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**.

Información relacionada

Directivas de alerta
Reenvío de registros de auditoría a servidores remotos de Syslog

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 Habilitar políticas de alerta.
   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 Syslog.
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

Eliminar políticas de alerta
Inhabilitar políticas de alerta
Habilitar políticas de alerta
Editar políticas de alerta
Crear políticas de alerta
Administrar registros de auditoría

Configurar alertas de SMTP, SNMP y Syslog

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 SNMP y las propiedades 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:

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 **Habilitar autenticación** y luego 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. Haga clic en **Aplicar**.
7. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para configurar el reenvío de una captura SNMP:

1. Expanda **Configuración de 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.
4. Seleccione la versión de SNMP en el menú desplegable **VERSIÓN DE SNMP**. En la actualidad, solo se admiten las versiones SNMP1 y SNMP2.
5. En el cuadro **CADENA DE COMUNIDAD**, ingrese la cadena de comunidad SNMP del dispositivo que debe recibir la alerta.
6. El número de puerto predeterminado para las capturas SNMP es 162. Edite según sea necesario. Consulte Protocolos y puertos admitidos en OpenManage Enterprise.

7. Para probar un mensaje SNMP, haga clic en el botón **Enviar** de la captura correspondiente.
8. Haga clic en **Aplicar**. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para configurar los mensajes de Syslog:

1. Expanda **Configuración 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.
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 captura SNMP, puede ejecutar un script en OpenManage Enterprise para configurar una política que abre una incidencia en el sistema de incidencias de terceros para la administración de alertas. Puede crear y almacenar únicamente cuatro comandos remotos para ejecutar de inmediato o más adelante.

1. Haga clic en **Configuración de la aplicaciónEjecución del script**.
2. Ingrese lo siguiente en el cuadro de diálogo **Configuración de comandos remotos**:
   a) Nombre del script creado en el host remoto.
   b) Dirección IP del servidor de host remoto que ejecuta el comando.
   c) Para iniciar sesión en el servidor de host remoto:
      - Introduzca el nombre de usuario.
      - Ingrese la contraseña o una clave SSH. Proporcione una clave privada para la ejecución del script remoto. Para generar una clave privada, ejecute el siguiente comando en el host remoto:`ssh -keygen -t rsa`. La clave privada se almacena en la siguiente carpeta predeterminada: `cd /root/ .ssh/`.

   d) Comando que se debe ejecutar en el servidor de host remoto para abrir una incidencia. Comando de ejemplo: `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`
3. Haga clic en **Guardar**.

   Se guarda el comando. También puede definir y ejecutar estos comandos cuando establezca las directivas de alertas. Consulte Creación de directivas de alertas.

   NOTA:
   - **Puede ejecutar solo un archivo ejecutable o una secuencia de comandos a la vez.**
   - **El archivo ejecutable o la secuencia de comandos se pueden guardar en un servidor que OpenManage Enterprise no necesariamente detecte ni administre.**
   - **La secuencia de comandos puede tener un máximo de 1024 caracteres.**
   - **OpenManage Enterprise admite la sustitución de un token que puede resultar útil para la secuencia de comandos o el sistema de incidencias. Tokens admitidos: `$IP`, `$MSG`, `$HOSTNAME`, `$SEVERITY`, `$SERVICETAG`, `$RESOLUTION`, `$CATEGORY`, `$ASSETTAG`, `$DATE`, `$TIME` y `$MODEL`.**
   - **Si se ingresa un tipo de token no válido, aparece en blanco la salida.**

Habilitar políticas de alerta

Solo puede habilitar una directiva de alerta si esta se encuentra deshabilitada. Para habilitar una directiva de alerta mientras crea una directiva de alerta, seleccione la casilla de verificación **Habilitar política** en la sección **Nombre y descripción**. Consulte Crear políticas de alerta.

Para habilitar una directiva de alerta, seleccione la casilla de verificación correspondiente y haga clic en **Habilitar**. La directiva de alerta queda habilitada y aparece una marca visto que indica que está habilitada (columna **HABILITADA**).

NOTA: Para habilitar varias directivas de alerta a la vez, seleccione 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.

NOTA: El botón Habilitar de una directiva de alerta que ya esté habilitada se ve atenuado.

Información relacionada

Directivas de alerta

Reenvío de registros de auditoría a servidores remotos de Syslog

Editar políticas de alerta

1. Seleccione la casilla de verificación correspondiente a la directiva de alerta y haga clic en **Editar**.
2. En el cuadro de diálogo **Crear directiva de alerta**, edite las propiedades de la directiva de alerta.
   Para navegar por diferentes secciones en el cuadro de diálogo, consulte Crear políticas de alerta.

Información relacionada

Directivas de alerta

Reenvío de registros de auditoría a servidores remotos de Syslog

Inhabilitar políticas de alerta

Solo puede deshabilitar una directiva de alerta si esta se encuentra habilitada. Una directiva de alerta se deshabilita cuando se crea una directiva de alerta desmarcando la casilla de verificación **Habilitar directiva** en la sección **Nombre y descripción**. Consulte Crear políticas de alerta.

Para deshabilitar una directiva de alerta, seleccione la casilla de verificación correspondiente a la directiva de alerta y haga clic en **Deshabilitar**. La directiva de alerta queda deshabilitada y se elimina la marca visto que indica que está habilitada (columna **HABILITADO**).

NOTA: Puede deshabilitar varias directivas de alerta al mismo tiempo 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. Sin embargo, una directiva de alerta debe tener al menos una acción asociada a él.

NOTA: El botón Deshabilitar de una directiva de alerta que ya está deshabilitada se ve atenuado.

Información relacionada

Directivas de alerta

Reenvío de registros de auditoría a servidores remotos de Syslog

Eliminar políticas de alerta

Para eliminar una directiva de alerta, seleccione la casilla de verificación correspondiente a la directiva de alerta y, a continuación, haga clic en **Eliminar**. De este modo, se elimina y se retira la directiva de alerta de la tabla **Directivas de alerta**.

NOTA: 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.

Información relacionada

Directivas de alerta

Reenvío de registros de auditoría a servidores remotos de Syslog

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.

12

Administrar registros de auditoría

Los registros de auditoría indican las acciones que se han realizado en los dispositivos que supervisa OpenManage Enterprise. Los datos de registro lo ayudan a usted o a los equipos de soporte de Dell EMC a solucionar problemas o ejecutar análisis. Los archivos de registro de auditoría se pueden exportar a formatos de archivo .CSV. Consulte Exportar todos los datos o aquellos seleccionados.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Si hace clic en **OpenManage Enterprise** y selecciona los elementos que se encuentran en **Supervisión**, puede:

- Crear trabajos para controlar el estado de alimentación del dispositivo y los LED del dispositivo. Consulte Utilización de trabajos para el control de dispositivos.
- Detectar y administrar dispositivos. Consulte Detección de dispositivos.
- Programar trabajos para generar un inventario de dispositivos. Consulte Administración del inventario del dispositivo.
- Crear y recibir alertas sobre la garantía de los dispositivos. Consulte Administración de garantía de dispositivos.
- Crear informes sobre los componentes de los dispositivos. Consulte Generación de informes de rendimiento de dispositivos.
- Administrar MIB. Consulte Administración de MIB.

NOTA: 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.**

1. Seleccione **Supervisión** > **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.
   - **Hora de inicio** y **Hora de finalización**: seleccione la hora aproximada de inicio y finalización cuando se realizó la tarea.
   - **Usuario**: ingrese el usuario de OpenManage Enterprise que realizó la tarea.
   - **Dirección de origen**: ingrese la dirección IP del sistema.
   - **Categoría**: seleccione una categoría a la que pertenece la tarea. De esta forma, se muestran todos los mensajes en dicha categoría.
   - **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.
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 en el . Sin embargo, en todas las versiones de chasis VRTX y FX2, aparece la fecha correcta.

Información relacionada

Reenvío de registros de auditoría a servidores remotos de Syslog

Temas:

- Reenvío de registros de auditoría a servidores remotos de Syslog

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 Habilitar políticas de alerta.
   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 Syslog.
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

Eliminar políticas de alerta
Inhabilitar políticas de alerta
Habilitar políticas de alerta
Editar políticas de alerta
Crear políticas de alerta
Administrar registros de auditoría

13

Utilización de trabajos para el control de dispositivos

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: Cada tipo de trabajo se limita a los dispositivos que:

- **El usuario tenga permisos de acceso.**
- **Tenga la capacidad de completar la acción necesaria.**

Esta regla se aplica a todas las tareas tales como parpadear, control de alimentación, administración de líneas base del firmware y administración de la línea base de cumplimiento de la configuración, en las que está involucrada la tarea de selección de dispositivos.

Haciendo clic en **OpenManage Enterprise** > **Supervisión** > **Trabajos**, puede:

- 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, 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 Visualización y configuración de dispositivos.
- Ejecutar el trabajo seleccionando la casilla de verificación correspondiente a un trabajo y haciendo clic en **Ejecutar ahora**.
- Detener el trabajo seleccionando la casilla de verificación correspondiente a un trabajo y haciendo clic en **Detener**.
- Habilitar el trabajo seleccionando la casilla de verificación correspondiente a un trabajo y haciendo clic en **Habilitar**.
- Deshabilitar un trabajo seleccionando la casilla de verificación correspondiente a un trabajo y haciendo clic en **Deshabilitar**.
- Eliminar un trabajo seleccionando la casilla de verificación correspondiente a un trabajo y haciendo clic en **Eliminar**.

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 la lista de trabajos

Haga clic en **OpenManage Enterprise** > **Supervisión** > **Trabajos**, para ver la lista de trabajos existentes. Se muestra información como estado del trabajo, tipo de trabajo y fecha y hora. 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. Los estados de un trabajo son:

- Nuevo: el trabajo se ha creado, pero no se ha ejecutado aún. Para ejecutar un trabajo, seleccione la casilla de verificación correspondiente y haga clic en **Ejecutar ahora**. El trabajo se inicia y la columna **ESTADO DEL TRABAJO** indica el estado como **En ejecución**.
- En ejecución
- Programado
- Completo
- Finalizado con errores
- En error

- Detenido

Un trabajo pertenece a cualquiera de los siguientes tipos:

- **Condición**: obtiene el estado de la condición de un dispositivo. Consulte Estados de los dispositivos.
- **Inventario**: crea el informe de inventario de un dispositivo. Consulte Administración del inventario del dispositivo.
- **Configuración de dispositivos**: crea la línea base de cumplimiento de configuración del dispositivo. Consulte Administración del cumplimiento de la configuración del dispositivo.
- **Report_Task**: crea informes acerca de los dispositivos mediante el uso de campos de datos integrados o personalizados. Consulte Informes.
- **Garantía**: genera datos acerca del estado de garantía de los dispositivos. Consulte Administración de la garantía del dispositivo.
- **Onboarding_Task**: consulte Incorporación de dispositivos.
- **Detección**: detecte los dispositivos que se administrarán con OpenManage Enterprise. Consulte Detección de dispositivos para la supervisión o administración.

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.

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.

NOTA: De forma predeterminada, solo está habilitada para crear nuevos trabajos la pestaña Crear. Sin embargo, si selecciona un trabajo desde la lista, las pestañas ejecutar, eliminar, habilitar, detener y deshabilitar un trabajo están habilitadas.

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.

Crear un trabajo para hacer parpadear los LED del dispositivo

1. Haga clic en **Crear** y, a continuación, seleccione **Hacer parpadear los dispositivos**.
2. En el cuadro de diálogo **Asistente para hacer parpadear los dispositivos**:
   a) En la sección **Opciones**:
      1. En la casilla **Nombre del trabajo**, ingrese el nombre del trabajo.
      2. 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.
      3. 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.
   c) En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos.
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 de trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte Visualizar la información de trabajos individuales.

Crear un trabajo para administrar dispositivos de alimentación

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**:
      1. Ingrese el nombre del trabajo en **Nombre del trabajo**.
      2. En el menú desplegable **Opciones de alimentación**, seleccione cualquiera de las tareas: **Encender**, **Apagar** o **Realizar el ciclo de apagado y encendido**.
      3. 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.
   c) En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos.
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.

Crear un trabajo de comando remoto para la administración de dispositivos

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 la casilla **Argumentos**, ingrese el comando y, a continuación, haga clic en **Siguiente**.
   Una marca visto verde junto a **Opciones** indica que se han proporcionado los datos necesarios.
   NOTA: No ejecute el comando RACADM `raclog` en el cuadro de diálogo Asistente para trabajos de línea de comandos. Consulte los datos de registro de hardware del dispositivo en la lengüeta Registros de hardware.
3. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino.
4. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos.
5. Haga clic en **Finalizar**.
   El trabajo se crea y aparece en la lista 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.

Cambiar el tipo de complemento de consola virtual

Si la versión del complemento que utiliza el servidor es anterior a HTML5, se muestra un mensaje que solicita que actualice el tipo de complemento. Para actualizar, haga clic en **CAMBIAR A HTML5** y, a continuación, realice lo siguiente:

1. Haga clic en **Crear** y, a continuación, seleccione **Cambiar complemento de la consola virtual en los dispositivos**.
2. 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**.
3. En la sección **Destino del trabajo**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte Seleccionar dispositivos y grupos de dispositivos de destino.
   a) Haga clic en **Siguiente**.
4. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte Definiciones de los campos Programar trabajos.
5. Haga clic en **Finalizar**.
   El trabajo se crea y aparece en la lista 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.

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**.

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 Lista de dispositivos. Para obtener información acerca de los grupos de dispositivos, consulte Organizar los dispositivos en grupos.
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.

14

Detección de dispositivos para la supervisión o administración

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Si hace clic en **OpenManage EnterpriseSupervisiónDetección**, 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: El chasis MX7000 no se detecta cuando intenta realizar la detección usando la versión OpenManage Enterprise: TechRelease. Después de que actualice a la versión 3.1 de OpenManage Enterprise, se detectará el mismo chasis MX7000. Sin embargo, las funciones disponibles son limitadas. Se recomienda crear una tarea de detección del chasis MX7000 en la versión 3.1 de OpenManage Enterprise después de finalizar la actualización.

NOTA: 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.

NOTA: 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.

Con la característica de detección, puede:

- Ver, agregar y quitar dispositivos de la lista de exclusión global. Consulte Dispositivos de exclusión global.
- Crear, ejecutar, editar, eliminar y detener los trabajos de detección de dispositivos.

Tareas relacionadas

Eliminar un trabajo de detección de dispositivos
Visualizar los detalles del trabajo de detección de dispositivos
Detener un trabajo de detección de dispositivos
Ejecutar un trabajo de detección de dispositivos
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 almacenamiento de Dell y switch de red
Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP
Especificar el modo de detección para crear VARIOS trabajos de detección
Editar un trabajo de detección de dispositivos

Temas:

- 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
- Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell y switch de red
- 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
- Activar el modo WS-Man en HTTPS para detectar servidores Windows o Hyper-V

Crear un trabajo de detección de dispositivos

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Para detectar un dispositivo:

1. Haga clic en **Monitor** > **Detección** > **Crear**.
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: 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 va a detectar más de 8000 dispositivos a la vez, se recomienda que ingrese un rango de IP para detectarlos con una cantidad menor de trabajos de detección y, por consiguiente, evitar la creación de varios trabajos. Ingresar direcciones IP individuales no se recomienda para la detección de una gran cantidad de 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.
   - 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 conmutador de red, seleccione **ALMACENAMIENTO DE DELL** o **CONMUTADOR 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.
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**.
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.
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.
9. 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 Syslog. Si selecciona esta opción, pero no se configura SMTP, no se muestra el botón **Terminar** para continuar con la tarea.
10. Haga clic en **Finalizar**. No se muestra el botón Terminar 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.

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 E/S 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.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 Privilegios de usuario de OpenManage Enterprise basados en el rol.
   - 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 se registró con el dispositivo como receptor de alertas.
2. En el panel de trabajo, seleccione la casilla de verificación correspondiente a los dispositivos y haga clic en **Más accionesIncorporación**.
   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.

Tabla 12. Matriz de compatibilidad de protocolos para detección

	Protocolos					
Dispositivo/ sistema operativo	**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)**
iDRAC6 o posteriores	Compatible	Compatible	No compatible	No compatible	No compatible	No compatible
PowerEdge C *	Compatible	Compatible	No compatible	No compatible	No compatible	No compatible
Chasis PowerEdge (CMC)	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
Dispositivos de almacenamiento	No compatible	No compatible	Compatible	No compatible	No compatible	No compatible
Conmutadores de Ethernet	No compatible	No compatible	Compatible	No compatible	No compatible	No compatible
ESXi	No compatible	No compatible	No compatible	No compatible	No compatible	Compatible
Linux	No compatible	No compatible	No compatible	Compatible	No compatible	No compatible
Windows (Hyper-V)	Compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Servidores que no son Dell	No compatible	No compatible	No compatible	No compatible	Compatible	No 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.

Información relacionada

Detección de dispositivos para la supervisión o administración

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

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

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

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.

Dispositivos de exclusión global

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.

Cuando se detectan dispositivos desde todos los dispositivos disponibles, puede excluir algunos dispositivos de la supervisión de OpenManage Enterprise como se indica a continuación:

1. 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.
2. Haga clic en **Agregar**.
3. 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 ver la lista de dispositivos globalmente excluidos, haga clic en:

   - **Dispositivos** > **Todos los dispositivos** > **Excluir globalmente**. El cuadro de diálogo **Exclusión global de rangos** muestra la lista de dispositivos excluidos.
   - **Monitor** > **Detección** > **Crear** > **Excluir globalmente**. El cuadro de diálogo **Exclusión global de rangos** muestra la lista de dispositivos excluidos.
   - **Monitor** > **Detección** > **Lista de exclusión global**. El cuadro de diálogo **Exclusión global de rangos** muestra la lista de dispositivos excluidos.

   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.

NOTA: 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 y chasis.
7. Programe el trabajo de detección. Consulte Definiciones de los campos Programar trabajos.
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

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

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

1. Seleccione la casilla de verificación **Detectar usando WS-Man/Redfish (iDRAC, servidor o chasis)** para detectar servidores.

   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 servidor que se debe 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.

      - **Generar clave de confianza**: Desactivada de manera predeterminada. Seleccione esta opción para generar una clave de confianza de dispositivos para la comunicación con los dispositivos.

        NOTA: Por primera vez, un usuario debe generar la clave de confianza mediante el uso de la API de REST, solo después de la cual se puede utilizar esta opción. Esta clave se genera por dispositivo y permite establecer una relación de confianza con el dispositivo administrado.

   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**. Solo se aplica a los chasis CMC VRTX, M1000e y FX2. En el caso del chasis MX7000, los módulos de E/S se detectan automáticamente.
5. Seleccione una de las siguientes casillas de verificación para activar la detección usando estos protocolos. Escriba las credenciales correspondientes del dispositivo:

   - **Activar SNMP**: para detección de dispositivos compatibles con SNMP.
   - **Activar RedFish**: para detección de servidores.
   - **Activar IPMI**: para detección de servidores.
   - **Activar SSH**: para detección de los servidores Linux.
   - **Activar VMware**: para detección de los hosts ESXi.
6. Haga clic en **Finalizar**.
7. Realice las tareas en Crear un trabajo de detección de dispositivos.

Información relacionada

Detección de dispositivos para la supervisión o administración

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 haciendo clic en **Configuración adicional**, consulte Creación de plantillas personalizadas de trabajos de detección de dispositivos para servidores y chasis.

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.

Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell y switch de red

1. En el menú desplegable **Tipo de dispositivo**, seleccione **ALMACENAMIENTO DE DELL** o **SWITCH DE RED**.
   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**, ingrese la versión de SNMP del dispositivo que se debe detectar.
4. Ingrese el tipo de comunidad.
5. Para crear plantillas de detección personalizadas (para los dispositivos SNMP, como para almacenamiento y redes) haciendo clic en **Configuración adicional**, consulte Creación de plantillas personalizadas de trabajos de detección de dispositivos para dispositivos SNMP.
6. Realice las tareas en Crear un trabajo de detección de dispositivos.

Información relacionada

Detección de dispositivos para la supervisión o administración

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.

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

Información relacionada

Detección de dispositivos para la supervisión o administración

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.

Información relacionada

Detección de dispositivos para la supervisión o administración

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

Activar el modo WS-Man en HTTPS para detectar servidores Windows o Hyper-V

De manera predeterminada, el servicio WS-Man no está activado en los servidores Windows. Debe desactivar el servicio WS-Man en los servidores de destino en el modo HTTPS.

Requisitos previos:

- IIS con HTTPS desactivado
- Servicio WS-Man con HTTPS desactivado
- PowerShell 4.0 para configurar el servicio WS-Man con certificado

Creación de un certificado Self-Sign

NOTA: Si tiene un certificado firmado públicamente, las cosas se simplifican más y puede usar Set-WSManQuickConfig -UseSSL. Ejecute el siguiente comando en PowerShell iniciando sesión como administrador:

```
$Cert = New-SelfSignedCertificate -CertstoreLocation Cert:\LocalMachine\My -DnsName "myHost"
```

Es importante ingresar el nombre del servidor que desea administrar de manera remota a el parámetro -DnsName. Si el servidor tiene un nombre DNS, debe utilizar el nombre de dominio calificado completamente (FQDN).

NOTA: La variable $Cert es importante porque almacena huella digital para usar el comando posteriormente.

Crear una comunicación remota con PowerShell en el sistema host

El comando Enable-PSRemoting también inicia un oyente de WS-Man, pero solo para HTTP.

```
Enable-PSRemoting -SkipNetworkProfileCheck -Force
```

1. Si no desea que alguien utilice HTTP para conectarse al servidor, puede eliminar el oyente HTTP ejecutando el comando:

   ```
   Get-ChildItem WSMan:\Localhost\listener | Where -Property Keys -eq "Transport=HTTP" |
   Remove-Item -Recurse
   ```

2. Quite todos los oyentes de WS-Man para agregar el oyente de HTTPS nuevo:

   ```
   Remove-Item -Path WSMan:\Localhost\listener\listener* -Recurse
   ```

3. Agregue su oyente HTTPS de WS-Man:

   ```
   New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -
   CertificateThumbPrint $Cert.Thumbprint -Force
   ```

   NOTA: Utilice la variable $Cert que definió anteriormente para leer la huella digital. Esta variable permite que New-Item cmdlet encuentre el certificado en el almacén de certificados.

4. Agregar la regla de firewall:

   ```
   New-NetFirewallRule -DisplayName "Windows Remote Management (HTTPS-In)" -Name "Windows
   Remote Management (HTTPS-In)" -Profile Any -LocalPort 5986 -Protocol TCP
   ```

5. Verificar los valores mediante la ejecución del siguiente comando:

   ```
   C:\Windows\system32>winrm g winrm/config
   Config
       MaxEnvelopeSizekb = 500
       MaxTimeoutms = 60000
       MaxBatchItems = 32000
       MaxProviderRequests = 4294967295
       Client
           NetworkDelayms = 5000
           URLPrefix = wsman
           AllowUnencrypted = false
           Auth
               Basic = true
               Digest = true
               Kerberos = true
               Negotiate = true
               Certificate = true
               CredSSP = false
           DefaultPorts
               HTTP = 5985
               HTTPS = 5986
           TrustedHosts
       Service
           RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
           MaxConcurrentOperations = 4294967295
           MaxConcurrentOperationsPerUser = 1500
           EnumerationTimeoutms = 240000
           MaxConnections = 300
           MaxPacketRetrievalTimeSeconds = 120
           AllowUnencrypted = false
           Auth
               Basic = true
               Kerberos = true
               Negotiate = true
               Certificate = false
               CredSSP = false
               CbtHardeningLevel = Relaxed
           DefaultPorts
               HTTP = 5985
               HTTPS = 5986
           IPv4Filter = *
           IPv6Filter = *
   ```

```
        EnableCompatibilityHttpListener = false
        EnableCompatibilityHttpsListener = true
        CertificateThumbprint = 02554D694FD06BB3C765E5868EFB59B7D786ED67
        AllowRemoteAccess = true
    Winrs
        AllowRemoteShellAccess = true
        IdleTimeout = 7200000
        MaxConcurrentUsers = 2147483647
        MaxShellRunTime = 2147483647
        MaxProcessesPerShell = 2147483647
        MaxMemoryPerShellMB = 2147483647
        MaxShellsPerUser = 2147483647
```

NOTA: Si `service-basic-authentication` es falso, ejecute el siguiente comando:

```
winrm set winrm/config/service/auth @{Basic="true"}
```

NOTA: En la configuración de WinRM, active HTTPS mediante la ejecución del comando:

```
winrm set winrm/config/service @{EnableCompatibilityHttpsListener="true"}
```

6. **Activación de IIS para aceptar HTTPS en 443**: ejecute el siguiente comando en el servidor Hyper-V desde un sistema remoto para asegurarse de que los valores de configuración funciona:

```
winrm e wmi/root/virtualization/v2/Msvm_SummaryInformation  -r:https://<hyper-v server
ip>:443/wsman -u:UserName -p:password -skipCNcheck -skipCAcheck -skipRevocationcheck -
a:Basic
```

7. Inicie el Administrador de IIS.
8. En el cuadro de diálogo **Vinculaciones de sitios en sitio web predeterminado**, ingrese `443` como el número de puerto HTTPS.
9. Seleccione el certificado SSL que se crea en PowerShell iniciando sesión como administrador.

15

Administración del inventario del dispositivo

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.

Tareas relacionadas

Ejecución de un trabajo de inventario ahora
Detención de un trabajo de inventario
Eliminación de un trabajo de inventario
Creación de un trabajo de inventario

Temas:

Creación de un trabajo de inventario

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

1. 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.
   Para obtener información acerca de los grupos de dispositivos, consulte Organizar los dispositivos en grupos.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior.
   Consulte Definiciones de los campos Programar trabajos.

5. Para generar un inventario de la línea base de cumplimiento de configuración, seleccione la casilla de verificación **Ejecutar adicionalmente el inventario de configuración**.

   Para obtener información acerca de las líneas base de cumplimiento de configuración, consulte Administración del cumplimiento de la configuración del dispositivo.
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.

Información relacionada

Administración del inventario del dispositivo

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

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

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

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.
   La tarea del programa de inventario se actualiza y aparece en la tabla.

16

Administración de la garantía del dispositivo

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Haciendo clic en **OpenManage Enterprise** > **Supervisión** > **Garantía**, puede ver los estados de garantía de los dispositivos supervisados por OpenManage Enterprise. Tiene la posibilidad de exportar todos los datos o aquellos seleccionados a una hoja de Excel para fines estadísticos y de análisis. En el panel derecho, si hace clic en **Renovación de garantía de Dell para dispositivo**, será redirigido al sitio de soporte de Dell EMC para habilitarlo para que administre la garantía del dispositivo. En la página de garantía, junto con el estado de garantía y la etiqueta de servicio, se muestra la siguiente información.

- La etiqueta de servicio, el nombre del modelo y el tipo de modelo del dispositivo.
- **TIPO DE GARANTÍA**:
  - Inicial: la garantía sigue siendo válida mediante la garantía proporcionada cuando se adquirió por primera vez OpenManage Enterprise.
  - Extendida: la garantía se extiende porque caducó la duración de la garantía proporcionada cuando se adquirió por primera vez OpenManage Enterprise.
- **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.

OpenManage Enterprise ofrece un informe incorporado sobre las garantías que vencen en los próximos 30 días. Haga clic en **OpenManage Enterprise** > **Supervisiòn** > **Informes** > **Garantías que vencen en los próximos 30 días**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

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 interfaz gráfica de usuario de OpenManage Enterprise. Para actualizar los datos de la tabla, haga clic en **Actualizar la 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.

Tareas relacionadas

Visualización de información de garantía del dispositivo

Temas:

Visualización de información de garantía del dispositivo

Haga clic en **OpenManage Enterprise** > **Supervisión** > **Garantía**. Se muestra una lista de dispositivos y su etiqueta de servicio, modelo, tipo, garantía asociada e información de nivel de servicio. Para ver una síntesis rápida de los dispositivos cuyo estado de garantía está por caducar, consulte Administrar la garantía del dispositivo utilizando el tablero de OpenManage Enterprise.

- Para ver descripciones de campos, consulte Administración de garantía de dispositivos.
- Para ver la información de la garantía de un dispositivo, seleccione la casilla de verificación correspondiente al dispositivo. La información de la garantía aparece en el panel derecho. Junto con la demás información, aparecen el código de nivel de servicio, el proveedor de servicios y la fecha de inicio y finalización de la garantía.
- Si hace clic en **Renovación de garantía de Dell para dispositivo**, será redirigido al sitio de soporte de Dell EMC para habilitarlo para que administre la garantía.
- Para ordenar los datos de la tabla en función de una columna, haga clic en el título de la columna.
- En la esquina superior derecha, haga clic en el botón **Actualizar la garantía** para actualizar los datos que aparecen en la tabla de la garantía.
- Para buscar un dispositivo, utilice la opción **Filtros avanzado**.

Información relacionada

Administración de la garantía del dispositivo

17

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.

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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

NOTA: Los datos que se le muestran en un informe dependen de los privilegios que tenga en OpenManage Enterprise. Por ejemplo, cuando se genera un informe, si no tiene permiso para ver un cierto grupo de dispositivos, los datos de ese grupo no se muestran en su caso.

Tabla 13. 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

Actualmente, se pueden generar los siguientes informes incorporados para extraer información sobre lo siguiente:

- Categoría de dispositivo: activo, FRU, firmware, cumplimiento del firmware, 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
Generación de informes y su envío a través de correo electrónico
Editar informes
Eliminar informes

Temas:

Ejecutar informes

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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. 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.

NOTA: No se recomienda ejecutar informes con frecuencia, ya que consume recursos de datos y de procesamiento.

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.

NOTA: 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 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.

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

Generación de informes y su envío a través de correo electrónico

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. Puede enviar informes por correo electrónicos de 20 a 30 destinatarios a la vez. 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.
   c) Haga clic en **Finalizar**.
   El informe se envía por correo electrónico y se registra en los registros de auditoría.

Información relacionada

Informes

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

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

Creación de informes

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 14. 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.
   b) Expanda el menú **Columnas**, y seleccione las casillas de verificación de los campos que deben aparecer como columnas en el informe.
   Los datos de estas columnas se completan según los criterios de filtro que haya definido.
4. Haga clic en **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. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Seleccionar los criterios de una consulta

Defina filtros cuando cree criterios de consulta para:

- Generación de informes personalizados. Consulte Creación de informes.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte Crear o editar un grupo de dispositivos de consulta.

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. El número de filtros predefinidos para cada consulta existente varía según el tipo de consulta. Por ejemplo, la consulta para **sistemas hipervisor** tiene 6 filtros predefinidos, mientras la consulta para **los conmutadores de red** tiene solo tres. Cuando se define una consulta, es posible definir un máximo de 20 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 Administrar registros de auditoría.

Información relacionada

Administración del cumplimiento de la configuración del dispositivo
Editar una línea base de cumplimiento de configuración
Eliminar una línea base de cumplimiento de configuración

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.

18

Administración de archivos de MIB

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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
- Eliminación de archivos de MIB
- Resolución de tipos de MIB

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 15. 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
- Edición de capturas de MIB
- Eliminación de archivos de MIB
- Resolución de tipos de MIB
- Descarga de un archivo de MIB de OpenManage Enterprise

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 necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.
   b) Haga clic en **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.
   - 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. 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 **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.

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.
   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.

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.

19

Administración de los ajustes del servidor OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.
- Configurar correos electrónicos, SNMP y propiedades de Syslog para la administración de alertas. Consulte Configurar alertas de SMTP, SNMP y Syslog.
- 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 Comprobación y actualización de la versión de OpenManage Enterprise.
- 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.

Tareas relacionadas

Eliminación de servicios de directorio

Temas:

- Configuración de credenciales de SNMP
- Administración de la configuración de garantía
- Comprobación y actualización de la versión de OpenManage Enterprise
- Ejecutar comandos y scripts remotos
- Configuración de OpenManage Mobile

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 Privilegios de usuario de OpenManage Enterprise basados en el rol.

NOTA: Si tiene más de una IP para OpenManage Enterprise mediante el uso de vNIC, solo debe usar la dirección IPv4 que se indica en el campo Dirección IP actual (haga clic en Configuración de la aplicaciónConfiguración actual) para acceder a la API de REST.

1. Para ver la configuración actual de la red de OpenManage Enterprise, como nombre de dominio DNS, FQDN y las configuraciones de IPv4 e IPv6, expanda **Configuración actual**.
2. Para configurar el tiempo de espera de la sesión actual de OpenManage Enterprise, expanda **Configuración del servidor web** e ingrese la duración del tiempo de espera de la sesión en minutos.

   Si el dispositivo está inactivo durante el tiempo ingresado, se finaliza la sesión. El usuario actual se desconecta automáticamente del dispositivo.
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) Haga clic en **Aplicar**.
   d) 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.

Administración de usuarios de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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). 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.

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Usuarios**, puede:

- Ver, agregar, habilitar, editar o eliminar usuarios de OpenManage Enterprise.
  NOTA: No se pueden habilitar, deshabilitar ni eliminar los usuarios de admin/sistema/root. Puede cambiar la contraseña haciendo clic en Editar en el panel derecho.
- Ver detalles sobre los usuarios conectados y, a continuación, finalizar (cerrar) una sesión de usuario.
- Administrar servicios de directorio.
- Importar y administrar usuarios de Active Directory.

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. 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 y Desactivación de usuarios de OpenManage Enterprise.
- **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.

Tareas relacionadas

Eliminación de servicios de directorio
Eliminación de usuarios de OpenManage Enterprise
Finalización de sesiones de usuario

Referencia relacionada

Desactivación de usuarios de OpenManage Enterprise
Activación de usuarios de OpenManage Enterprise

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
Eliminación de usuarios de OpenManage Enterprise
Finalización de sesiones de usuario

Información relacionada

Administración de usuarios de OpenManage Enterprise

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
Eliminación de usuarios de OpenManage Enterprise
Finalización de sesiones de usuario

Información relacionada

Administración de usuarios de OpenManage Enterprise

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**.

Referencia relacionada

Desactivación de usuarios de OpenManage Enterprise
Activación de usuarios de OpenManage Enterprise

Información relacionada

Administración de usuarios de OpenManage Enterprise

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**.

Referencia relacionada

Desactivación de usuarios de OpenManage Enterprise
Activación de usuarios de OpenManage Enterprise

Información relacionada

Administración de los ajustes del servidor OpenManage Enterprise
Administración de usuarios de OpenManage Enterprise

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.

Referencia relacionada

Desactivación de usuarios de OpenManage Enterprise

Activación de usuarios de OpenManage Enterprise

Información relacionada

Administración de usuarios de OpenManage Enterprise

Privilegios de usuario de OpenManage Enterprise basados en el rol

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. Este se conoce como Control de acceso basado en roles (RBAC). Se trata de una lista común de RBAC para los usuarios según sus roles y las funciones de OpenManage Enterprise. Sin embargo, cuando es necesario, se proporciona una lista de RBAC de usuario a nivel de tareas en las secciones respectivas para una referencia rápida. Por lo tanto, en la consola se aplica uno de los roles por cuenta. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte Administración de usuarios de OpenManage Enterprise.

Tabla 16. Privilegios de usuario basados en roles en OpenManage Enterprise

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Administrador	Administrador de dispositivos	Lector
Ejecutar informes	S	S	S
Ver	S	S	S
Administrar plantillas	S	S	N
Administrar la línea de base	S	S	N
Configurar el dispositivo	S	S	N
Actualizar el dispositivo	S	S	N
Administrar los trabajos	S	S	N
Crear supervisión de políticas	S	S	N
Implementar un SO	S	S	N
Control de alimentación	S	S	N
Administrar informes	S	S	N
Actualizar inventario	S	S	N
Configurar el dispositivo de OpenManage Enterprise	S	N	N
Administrar la detección	S	N	N
Administrar los grupos	S	N	N
Configurar la seguridad	S	N	N
Administrar capturas	S	N	N

Tareas relacionadas

Implementación y administración de OpenManage Enterprise

Referencia relacionada

Tipos de roles de usuario en OpenManage Enterprise

Adición y edición de usuarios de OpenManage Enterprise

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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). 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.

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 agregar usuarios de directorio, consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio.

1. Seleccione **Configuración de la aplicaciónUsuariosAgregar**.
2. En el cuadro de diálogo **Agregar nuevo usuario**:
   a) Ingrese la información del usuario.

      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.
   b) En el menú desplegable **Rol de usuario**, seleccione un rol:

      - **Administrador**
      - **Administrador de dispositivos**
      - **Lector**

      Para obtener más información, consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

      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.
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 de OpenManage Enterprise.
   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.

Importación de grupos de AD y LDAP

NOTA: Los usuarios con derechos de administrador no pueden activar ni desactivar usuarios de Active Directory (AD) ni de protocolo ligero de acceso a directorios (LDAP).

NOTA: Antes de importar grupos de AD en OpenManage Enterprise, debe incluir los grupos de usuarios en un GRUPO UNIVERSAL mientras configura el AD.

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.

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 Privilegios de usuario de OpenManage Enterprise basados en el rol.
   b) Haga clic en **Asignar**.
   Los usuarios de un grupo en el servicio de directorio seleccionado se asignan con las funciones del usuario seleccionado.

   NOTA: En el caso de grupos asignados al rol de Administrador de dispositivos (DM), la asignación del grupo para ese DM se debe completar después de terminar estas tareas mediante el uso de los pasos para editar un usuario local y asignar grupos para un administrador de dispositivos. Consulte Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio.
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, el usuario recibirá el rol de nivel más alto 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.

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. 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.
- Importe grupos de directorio y asigne todos los usuarios en el grupo para un rol específico. Consulte Importación de grupos de AD y LDAP.
- Para usuarios DM, edite el grupo de directorio para agregar los grupos que el DM puede administrar. Consulte Adición y edición de usuarios de OpenManage Enterprise.

Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio

1. Haga clic en **Configuración de la aplicaciónUsuariosServicios 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.

   a) Ingrese un nombre para el directorio 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.
   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.
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 aplicaciónUsuariosServicios 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.

   a) Ingrese un nombre 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) y la contraseña de la carpeta LDAP.
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.
   b) Para que coincida la configuración de LDAP en el servidor, escriba el DN de la base del grupo que desea buscar.
   c) Introduzca el atributo de usuario que se buscará. Si no está configurado, use UID. 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.
   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.
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 **Ok**.
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.

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 Privilegios de usuario de OpenManage Enterprise basados en el rol.

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 lector). 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.

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Seguridad**, puede proteger a OpenManage Enterprise mediante la especificación de un rango de direcciones IP de inicio de sesión o de una directiva de bloqueo de inicio de sesión.

- Expanda **Rango IP de inicio de sesión**:
  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 separadas por una coma.
  3. Haga clic en **Aplicar**. Para restablecer las propiedades predeterminadas, haga clic en **Descartar**.
- 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**.

Referencia relacionada

Certificados de seguridad

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 Privilegios de usuario de OpenManage Enterprise basados en el rol.

Para generar una solicitud de firma de certificado (CSR), consulte Generación y descarga de la solicitud de firma de certificado.

Información relacionada

Establecimiento de las propiedades de seguridad de inicio de sesión

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**.

Administración de preferencias de consola

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

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.

- Para establecer el número máximo de filas (informes) que se pueden ver en OpenManage empresa realice lo siguiente:
  1. Expanda la **Configuración del informe**.
  2. Ingrese un número en la casilla **Límite de filas de informes**. Número máximo de filas permitido=1000.
  3. Haga clic en **Aplicar**. Se ejecuta una tarea y se aplica el valor.
- 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, realice lo siguiente:
  1. Expanda **Condición de los dispositivos**.
  2. Ingrese la frecuencia con que se debe registrar la condición de los dispositivos y almacenar los datos.
  3. 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.
  4. Haga clic en **Aplicar**.
  5. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.
- Para establecer el modo mediante el cual se debe detectar el dispositivo. Por ejemplo, el nombre de DNS y el nombre de host:
  1. Expanda **Configuración de detección**.
  2. Para utilizar la configuración de DNS para detectar un dispositivo, seleccione la casilla de verificación **Preferir DNS**. Para NetBIOS, seleccione la casilla de verificación **Preferir NetBIOS**.
  3. Para utilizar el nombre de host del sistema en la detección de un dispositivo, seleccione la casilla de verificación **Preferir nombre del host del sistema**.
  4. Para detectar un dispositivo utilizando el nombre de host del sistema a través de iDRAC, seleccione la casilla de verificación **Preferir nombre de host de iDRAC**.
  5. Expanda **Configuración avanzada**:

- Ingrese uno o varios hostnames no válidos separados por comas para **Hostname de dispositivo no válido**. De manera predeterminada, se completa una lista de nombres de host no válidos del dispositivo.
- Ingrese las direcciones MAC comunes separadas por comas en **Direcciones MAC comunes**. De manera predeterminada, se completa una lista de direcciones MAC comunes.

6. Haga clic en **Aplicar**.
7. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

- Establezca los dispositivos que se deben mostrar en la vista **Todos los dispositivos**.

1. Expanda **Configuración de vista de todos los dispositivos**.
2. En el menú desplegable **Mostrar dispositivos desconocidos**, seleccione:
   - **Falso**: en la página Panel, no aparecen los dispositivos desconocidos en la lista de todos los dispositivos y grupos de dispositivos.
   - **Verdadero**: sí aparecen los dispositivos desconocidos en la lista.
3. Haga clic en **Aplicar**.
4. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

- En la sección **Configuración de SMB**, seleccione la versión del Bloque de mensaje de servidor (SMB) que debe usarse para la comunicación de red. La opción **Version2** (SMBv3) está activada en forma predeterminada.

  NOTA: Para activar SMBv1 o utilizar características como implementación de la plantilla o informes de diagnóstico, descargue desde el sitio dell.com.

- Para establecer la dirección del usuario que envía un mensaje de correo electrónico:

1. Expanda **Configuración de remitente de correo electrónico**.
2. Ingrese una dirección de correo electrónico y haga clic en **Aplicar**.

- Para establecer el formato de reenvío de capturas:

1. Expanda **Formato de reenvío de capturas**.
2. Para conservar los datos de la captura tal como se encuentran, seleccione **Formato original**. Para normalizar, seleccione **Normalizado**.
3. Haga clic en **Aplicar**.

Administración de alertas entrantes

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol.

Si hace clic en **OpenManage Enterprise Configuración de la aplicación** > **Alertas entrantes**, puede definir las propiedades del usuario que recibe las alertas entrantes mediante el protocolo SNMPv3. También puede establecer las propiedades de TrapForward.

- 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 161. 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 a la versión 3.1 de OpenManage Enterprise, 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.

- Para aplicar la configuración de TrapForward:
  1. Expanda **Configuración de TrapForward**.
     - Para reenviar la captura, seleccione **AS_IS**.
     - Para reenviar la captura normalizada, seleccione **Normalizada**.
  2. Haga clic en **Aplicar**.
  3. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

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

Si hace clic en **OpenManage Enterprise** > **Configuración de la aplicación** > **Configuración de la garantía**, puede activar la notificación de marcador de garantía que está presente en el encabezado de OpenManage Enterprise mediante los siguientes pasos. Todos los parámetros o configuración de esta página determinan la lógica del recuento del cuadro de mando para la garantía. De manera predeterminada, el usuario recibe un mensaje de alerta 90 días antes de la fecha de vencimiento de la garantía. Para editar el número de días:

1. Seleccione la casilla de verificación **Habilitar notificaciones por cuadro de mandos para garantía**.
2. Para editar este valor, escriba en la casilla **Fecha de vencimiento anterior a**. En el campo **Vencimiento de la garantía inferior a** en el panel de OpenManage Enterprise se muestran las garantías que coinciden con este criterio.
3. Para enviar un mensaje después de la fecha de vencimiento de la garantía, seleccione la casilla de verificación **Cuando se produzca el vencimiento de la garantía**. Cuando se selecciona esta opción, en el panel de OpenManage Enterprise (widgets) se muestra la cantidad de garantías que han vencido.
4. Haga clic en **Aplicar**.
   Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

   OpenManage Enterprise ofrece un informe incorporado sobre las garantías que vencen en los próximos 30 días. Haga clic en **OpenManage Enterprise** > **Supervisiòn** > **Informes** > **Garantías que vencen en los próximos 30 días**. Haga clic en **Ejecutar**. Consulte Ejecutar informes.

Comprobación y actualización de la versión de OpenManage Enterprise

Seleccione **Configuración de la aplicación Actualización de la consola** para ver la versión actual de OpenManage Enterprise, comprobar si está disponible una versión actualizada y luego actualizar la versión de OpenManage Enterprise.
A continuación, se muestra una lista de verificación que puede seguir para realizar tareas previas y posteriores a la actualización. Consulte Mapa de procesos para la comprobación y actualización de la versión de OpenManage Enterprise.

Información relacionada

Actualización de Dell.com
Actualización de un recurso compartido de red interna

Actualización de la versión OpenManage Enterprise

Se advierte automáticamente al usuario acerca de la disponibilidad de un nuevo paquete de actualización o de la información sobre la garantía en el portal de **Inicio**. Antes de actualizar a la versión más reciente, asegúrese de hacer lo siguiente:

- 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 ni tareas de implementación de dispositivos ni que se programen sus respectivas ejecuciones durante el tiempo de inactividad planificado.
- Notifique a los demás usuarios de la consola sobre la próxima actualización programada.
- Tome una instantánea de máquina virtual de la consola como copia de seguridad en caso de que ocurriera algo inesperado (Asigne tiempo de inactividad adicional para esta tarea, si fuera necesario).

NOTA: Antes de actualizar a OpenManage Enterprise versión 3.1, Dell EMC recomienda que la versión anterior de OpenManage Enterprise se configure con un mínimo de 16 GB de memoria. Para obtener más información, consulte Requisitos mínimos recomendados de hardware.

NOTA: Puede actualizar de OpenManage Enterprise - Tech Release u OpenManage Enterprise versión 3.0 a la versión 3.1 mediante el método Automático > En línea. Sin embargo, para actualizar de OpenManage Enterprise - Tech Release a OpenManage Enterprise versión 3.0, debe utilizar el método de actualización Manual > Fuera de línea.

NOTA: Si está disponible una versión actualizada de OpenManage Enterprise, aparecerá un mensaje en el panel. Los usuarios con todos los privilegios (administrador, administrador de dispositivos y lector) pueden ver el mensaje, pero solo un administrador puede optar por recibir recordatorios posteriores o descartar el mensaje.

NOTA: Cuando actualice OpenManage Enterprise-Tech Release a OpenManage Enterprise versión 3.1 y cuente con más de 5500 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.

Tabla 17. Privilegios de acceso basados en funciones para actualizar la versión de OpenManage Enterprise

El usuario con este rol...	Puede...
Administrador	Ver la versión actual de OpenManage Enterprise y actualizarla
Administrador de dispositivos y lector	Ver únicamente la versión actual de OpenManage Enterprise

NOTA: Para obtener más información sobre cómo actualizar OpenManage Enterprise a la versión más reciente, consulte el documento técnico *Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise* en el sitio de soporte.

Actualización de Dell.com

Debe asegurarse de que el dispositivo OpenManage Enterprise pueda acceder a Dell.com y a la actualización prevista.

1. Seleccione una de las siguientes opciones para mostrar información sobre una actualización disponible:
   - **Automática** y **En línea**: las actualizaciones se verifican automáticamente cada semana. Esta frecuencia no se puede modificar.
   - **Manual** y **En línea**: las actualizaciones se verifican cuando inicia manualmente la solicitud.
2. Haga clic en **Check Now** (Comprobar ahora).
   Se muestra la versión de actualización disponible con una breve descripción de las nuevas funciones.
3. Haga clic en **Actualizar ahora** y realice una actualización.

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.

NOTA: Después de que se haya actualizado correctamente la versión de OpenManage Enterprise, el estado del trabajo asociado de la página Detalles del trabajo se mostrará como Detenido. Sin embargo, significa que el estado del trabajo real se completó.

NOTA: Actualmente, no se crea un registro de auditoría después de que el proceso de actualización de la versión de OpenManage Enterprise finalice de forma correcta o incorrecta.

Tareas relacionadas

Comprobación y actualización de la versión de OpenManage Enterprise

Actualización de un recurso compartido de red interna

Debe configurar un recurso compartido 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: No se admite la actualización de OpenManage Enterprise versión 3.0 a la versión 3.1 mediante un recurso compartido de archivos de red (NFS). Para realizar la actualización, seleccione las opciones Automática y En línea o utilice los métodos HTTP y HTTPS. 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.

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 **Sin conexión**.
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: `http://<IP Address>/<Folder_Name>`, `http://<IP Address>/<Folder_Name>`, `https://<IP Address>/<Folder_Name>`.
   Se muestra la versión de actualización disponible con una breve descripción de las nuevas funciones.
4. Haga clic en **Actualizar ahora** y realice una actualización.

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.

NOTA: Después de que se haya actualizado correctamente la versión de OpenManage Enterprise, el estado del trabajo asociado de la página Detalles del trabajo se mostrará como Detenido. Sin embargo, significa que el estado del trabajo real se completó.

NOTA: Actualmente, no se crea un registro de auditoría después de que el proceso de actualización de la versión de OpenManage Enterprise finalice de forma correcta o incorrecta.

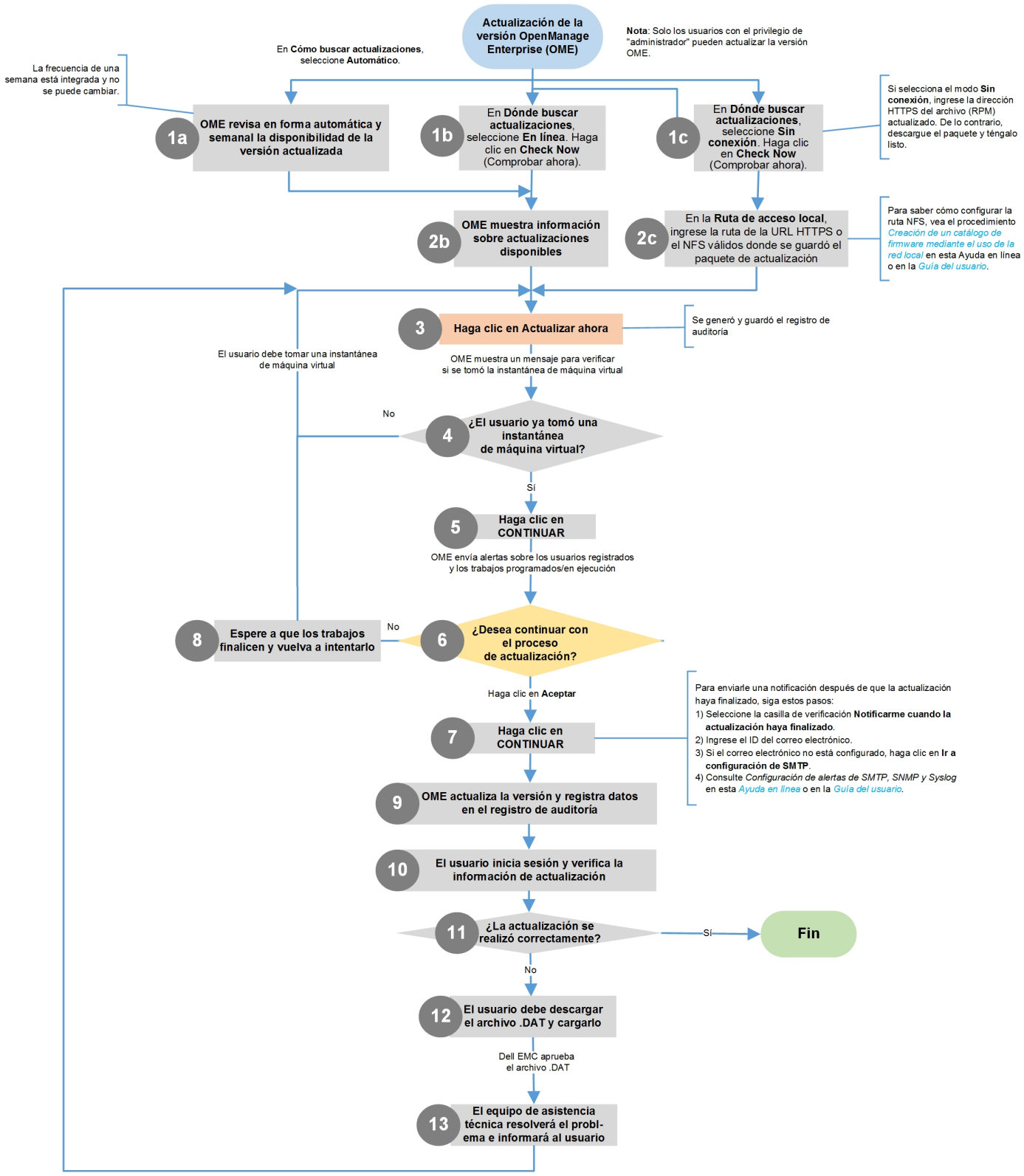
Tareas relacionadas

Comprobación y actualización de la versión de OpenManage Enterprise

Comprobación de actualizaciones OpenManage Enterprise VM

Consulte Comprobación y actualización de la versión de OpenManage Enterprise.

Mapa de procesos para la comprobación y actualización de la versión de OpenManage Enterprise



Información relacionada

Implementación y administración de OpenManage Enterprise

Ejecutar comandos y scripts remotos

Cuando recibe una captura SNMP, puede ejecutar un script en OpenManage Enterprise para configurar una política que abre una incidencia en el sistema de incidencias de terceros para la administración de alertas. Puede crear y almacenar únicamente cuatro comandos remotos para ejecutar de inmediato o más adelante.

1. Haga clic en **Configuración de la aplicaciónEjecución del script**.
2. Ingrese lo siguiente en el cuadro de diálogo **Configuración de comandos remotos**:
   a) Nombre del script creado en el host remoto.
   b) Dirección IP del servidor de host remoto que ejecuta el comando.
   c) Para iniciar sesión en el servidor de host remoto:
      - Introduzca el nombre de usuario.
      - Ingrese la contraseña o una clave SSH. Proporcione una clave privada para la ejecución del script remoto. Para generar una clave privada, ejecute el siguiente comando en el host remoto:`ssh -keygen -t rsa`. La clave privada se almacena en la siguiente carpeta predeterminada: `cd /root/ .ssh/`.
   d) Comando que se debe ejecutar en el servidor de host remoto para abrir una incidencia. Comando de ejemplo: `./RCE.sh $IP $MODEL $DATE $ASSETTAG $SERVICETAG`
3. Haga clic en **Guardar**.

   Se guarda el comando. También puede definir y ejecutar estos comandos cuando establezca las directivas de alertas. Consulte Creación de directivas de alertas.

NOTA:

- **Puede ejecutar solo un archivo ejecutable o una secuencia de comandos a la vez.**
- **El archivo ejecutable o la secuencia de comandos se pueden guardar en un servidor que OpenManage Enterprise no necesariamente detecte ni administre.**
- **La secuencia de comandos puede tener un máximo de 1024 caracteres.**
- **OpenManage Enterprise admite la sustitución de un token que puede resultar útil para la secuencia de comandos o el sistema de incidencias. Tokens admitidos: `$IP`, `$MSG`, `$HOSTNAME`, `$SEVERITY`, `$SERVICETAG`, `$RESOLUTION`, `$CATEGORY`, `$ASSETTAG`, `$DATE`, `$TIME` y `$MODEL`.**
- **Si se ingresa un tipo de token no válido, aparece en blanco la salida.**

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 emergentes 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 *OpenManage Mobile User's Guide* (Guía del usuario de OpenManage Mobile) en Dell.com/OpenManageManuals.

Tareas relacionadas

Activación o desactivación de notificaciones de alerta de OpenManage Mobile
Activación o desactivación de suscriptores de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile
Visualización del estado del servicio de notificación de alertas
Solución de problemas de OpenManage Mobile

Información relacionada

Activación o desactivación de notificaciones de alerta de OpenManage Mobile

Activación o desactivación de suscriptores de OpenManage Mobile
Solución de problemas de OpenManage Mobile

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

Información relacionada

Configuración de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile

Activación o desactivación de suscriptores de OpenManage Mobile

Las casillas de verificación de la columna **Activado** en la lista **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.

NOTA: 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.

NOTA: 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

Información relacionada

Configuración de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile

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
Activación o desactivación de suscriptores de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile
Visualización del estado del servicio de notificación de alertas

Información relacionada

Configuración de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile

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

Información relacionada

Configuración de OpenManage Mobile
Eliminación de un suscriptor de OpenManage Mobile
Visualización del estado del servicio de notificación de alertas

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 18. 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.**

Icono de estado	Descripción del estado
	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 19. 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 20. 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. 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

Información relacionada

Configuración de OpenManage Mobile

20

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 de una línea base de firmware.
- **CATÁLOGO**: el catálogo de firmware al cual pertenece la línea base de firmware. Consulte Administrar los catálogos de firmware.
- **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 de un dispositivo en comparación con su línea base.

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.

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.
2. Instalar o conceder archivo DAT.ini firmado de FSD. Consulte Instalar o conceder un archivo DAT.ini firmado de FSD.
3. Llamar FSD. Consulte Llamar FSD.
4. Desactivar FSD. Consulte Desactivar FSD.

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 LANZAMIENTO: fecha de lanzamiento del archivo de catálogo para su uso.