

Guía del usuario de Dell EMC OpenManage Enterprise, versión 3.4

Notas, precauciones y advertencias

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

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

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

Tabla de contenido

Lista de tablas.....	9
Capítulo1: Acerca de Dell EMC OpenManage Enterprise.....	11
Novedades de esta versión.....	12
Otra información útil.....	12
Cómo ponerse en contacto con Dell EMC.....	13
Licencia de OpenManage Enterprise Advanced.....	13
Funciones basadas en la licencia en OpenManage Enterprise.....	14
Capítulo2: Características de seguridad en OpenManage Enterprise.....	15
Privilegios de usuario de OpenManage Enterprise basados en el rol.....	15
Tipos de roles de usuario en OpenManage Enterprise.....	16
Capítulo3: Implementación y administración de OpenManage Enterprise.....	18
Prerrequisitos de instalación y requisitos mínimos.....	18
Requisitos mínimos recomendados de hardware.....	18
Requisitos mínimos del sistema para implementar OpenManage Enterprise.....	19
Implementar OpenManage Enterprise en VMware vSphere.....	19
Implementar OpenManage Enterprise en Hyper-V 2012 R2 y host anteriores.....	20
Implementar OpenManage Enterprise en un host de Hyper-V 2016.....	21
Implementar OpenManage Enterprise en un host de Hyper-V 2019.....	21
Implementación de OpenManage Enterprise utilizando una máquina virtual basada en kernel.....	22
Implementar mediante programación OpenManage Enterprise.....	23
Capítulo4: Introducción a OpenManage Enterprise.....	25
Iniciar sesión en OpenManage Enterprise.....	25
Configurar OpenManage Enterprise con interfaz de usuario de texto.....	25
Configurar OpenManage Enterprise.....	28
Configuración recomendada de escalabilidad y rendimiento para el uso óptimo de OpenManage Enterprise.....	28
Protocolos y puertos admitidos en OpenManage Enterprise.....	29
Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise.....	32
Capítulo5: Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise.....	33
Capítulo6: Portal de inicio de OpenManage Enterprise.....	35
Supervisión de dispositivos mediante el tablero de OpenManage Enterprise.....	35
Organizar los dispositivos en grupos.....	36
Gráfico de anillo.....	38
Estados de los dispositivos.....	39
Capítulo7: Administración de dispositivos.....	40
Organizar los dispositivos en grupos.....	41
Crear o eliminar un grupo estático de dispositivos.....	42

Crear o editar un grupo de dispositivos de consulta.....	43
Cómo agregar o editar dispositivos en un grupo estático secundario.....	44
Cambiar el nombre de los grupos secundarios que pertenecen a grupos estáticos o dinámicos de consulta..	45
Clonar un grupo estático o de consulta.....	45
Agregar dispositivos a un grupo nuevo.....	45
Agregar dispositivos a un grupo existente.....	45
Eliminar dispositivos de OpenManage Enterprise.....	46
Excluir dispositivos de OpenManage Enterprise.....	46
Actualizar el firmware y los controladores del dispositivo mediante las bases.....	46
Reversar la versión del firmware de un dispositivo individual.....	47
Actualizar el inventario de dispositivos.....	48
Actualizar el estado del dispositivo.....	48
Exportar el inventario de un solo dispositivo.....	49
Lista de dispositivos.....	49
Cómo realizar más acciones en el chasis y en los servidores.....	49
Información de hardware que se muestra para el chasis MX7000.....	50
Exportar todos los datos o aquellos seleccionados.....	50
Visualización y configuración de dispositivos.....	50
Descripción general del dispositivo.....	51
Información del hardware del dispositivo.....	51
Ejecutar y descargar informes de diagnóstico.....	52
Extraer y descargar informes de SupportAssist.....	53
Administración de los registros de hardware de dispositivos individuales.....	53
Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales.....	53
Iniciar la aplicación de administración iDRAC de un dispositivo.....	54
Iniciar la consola virtual.....	54
Capítulo8: Administrar el firmware y los controladores del dispositivo.....	55
Administrar catálogos de firmware y controladores.....	56
Agregar un catálogo con Dell.com.....	56
Agregar un catálogo a la red local.....	56
Información del certificado SSL.....	58
Actualizar un catálogo.....	58
Editar un catálogo.....	58
Eliminar un catálogo.....	58
Crear una base.....	59
Eliminar bases.....	59
Editar una base.....	60
Comprobar el cumplimiento del firmware y los controladores de un dispositivo.....	60
Ver el informe de cumplimiento de la base.....	60
Actualizar el firmware o los controladores con el informe de cumplimiento de la base.....	61
Capítulo9: Administrar las plantillas de configuración de dispositivos.....	64
Crear una plantilla desde un dispositivo de referencia.....	64
Crear una plantilla importando un archivo de plantilla.....	65
Ver la información de una plantilla.....	65
Editar una plantilla de servidor.....	66
Editar una plantilla de chasis.....	67
Editar plantilla de IOA.....	67

Editar las propiedades de red.....	67
Implementar las plantillas de dispositivos.....	68
Implementar las plantillas de IOA.....	69
Clonar plantillas.....	70
Implementación automática de la configuración en servidores o chasis que aún no se han descubierto.....	70
Crear destinos de implementación automática.....	70
Eliminar destinos de implementación automática.....	71
Exportar detalles del destino de implementación automática a diferentes formatos.....	72
Descripción general de la implementación sin estado.....	72
Administrar grupos de identidades: implementación sin estado.....	72
Crear grupo de identidades: información del grupo.....	72
Definir redes.....	77
Tipos de red.....	77
Editar o eliminar una red configurada.....	78
Exportar definiciones de VLAN.....	78
Importar definiciones de red.....	78
Capítulo10: Administrar perfiles.....	80
Crear perfiles.....	81
Ver detalles del perfil.....	81
Perfiles: ver red.....	82
Editar un perfil.....	82
Asignar un perfil.....	82
Anular asignación de perfiles.....	83
Volver a implementar perfiles.....	84
Migrar un perfil.....	84
Eliminar perfiles.....	85
Exportar datos de perfiles en formato HTML, CSV o PDF.....	85
Capítulo11: Administración del cumplimiento de la configuración del dispositivo.....	86
Administrar plantillas de línea base de cumplimiento.....	87
Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación.....	87
Crear una plantilla de línea base de cumplimiento a partir de un dispositivo de referencia.....	88
Crear una línea base de cumplimiento mediante la importación desde un archivo.....	88
Clonar una plantilla de línea base de cumplimiento.....	88
Editar una plantilla de cumplimiento de línea base.....	89
Crear la línea base de cumplimiento de una configuración.....	89
Editar una línea base de cumplimiento de configuración.....	90
Corrección de dispositivos no compatibles.....	91
Eliminar una línea base de cumplimiento de configuración.....	91
Capítulo12: Supervisión de alertas de dispositivos.....	93
Visualizar los registros de alertas.....	93
Confirmar alertas.....	94
No confirmar alertas.....	94
Ignorar alertas.....	94
Eliminar alertas.....	94
Visualizar las alertas archivadas.....	95
Descargar las alertas archivadas.....	95

Directivas de alerta.....	95
Crear políticas de alerta.....	97
Habilitar políticas de alerta.....	100
Editar políticas de alerta.....	100
Inhabilitar políticas de alerta.....	101
Eliminar políticas de alerta.....	101
Definiciones de alerta.....	101
Capítulo13: Administrar registros de auditoría.....	103
Reenvío de registros de auditoría a servidores remotos de Syslog.....	104
Capítulo14: Utilización de trabajos para el control de dispositivos.....	105
Ver la lista de trabajos.....	105
Visualizar la información de trabajos individuales.....	106
Crear un trabajo para hacer parpadear los LED del dispositivo.....	107
Crear un trabajo para administrar dispositivos de alimentación.....	107
Crear un trabajo de comando remoto para la administración de dispositivos.....	108
Crear un trabajo para cambiar el tipo de complemento de la consola virtual.....	108
Seleccionar dispositivos y grupos de dispositivos de destino.....	109
Capítulo15: Detección de dispositivos para la supervisión o administración.....	110
Detectar los servidores automáticamente mediante la función de descubrimiento iniciado por servidor.....	111
.....	112
Crear un trabajo de detección de dispositivos.....	112
Incorporación de dispositivos.....	114
Matriz de soporte de protocolos para detectar dispositivos.....	115
Visualizar los detalles del trabajo de detección de dispositivos.....	116
Editar un trabajo de detección de dispositivos.....	116
Ejecutar un trabajo de detección de dispositivos.....	116
Detener un trabajo de detección de dispositivos.....	116
Especificar varios dispositivos mediante la importación de datos desde el archivo .csv.....	117
Dispositivos de exclusión global.....	117
Especificar el modo de detección para crear un trabajo de detección de servidores.....	118
Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección.....	118
Especificar el modo de detección para crear un trabajo de detección de chasis.....	119
Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección.....	120
Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell.....	120
Especificar el modo de detección para crear un trabajo de detección de conmutadores de red.....	121
Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPS: configuración adicional para los protocolos de detección.....	121
Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP.....	121
Especificar el modo de detección para crear VARIOS trabajos de detección.....	122
Eliminar un trabajo de detección de dispositivos.....	122
Capítulo16: Administración del inventario del dispositivo.....	123
Creación de un trabajo de inventario.....	123
Ejecución de un trabajo de inventario ahora.....	124
Detención de un trabajo de inventario.....	124

Eliminación de un trabajo de inventario.....	124
Edición de un trabajo de programa de inventario.....	125
Capítulo17: Administración de la garantía del dispositivo.....	126
Ver y renovar la garantía del dispositivo.....	126
Capítulo18: Informes.....	128
Ejecutar informes.....	129
Generación de informes y su envío a través de correo electrónico.....	129
Editar informes.....	130
Copia de informes.....	130
Eliminar informes.....	130
Creación de informes.....	130
Seleccionar criterios de consulta durante la creación de informes.....	131
Exportación de informes seleccionados.....	132
Capítulo19: Administración de archivos de MIB.....	133
Importación de archivos de MIB.....	133
Edición de capturas de MIB.....	134
Eliminación de archivos de MIB.....	135
Resolución de tipos de MIB.....	135
Descarga de un archivo de MIB de OpenManage Enterprise.....	135
Capítulo20: Administración de los ajustes del servidor OpenManage Enterprise.....	136
Configurar los ajustes de la red de OpenManage Enterprise.....	137
Administración de usuarios de OpenManage Enterprise.....	138
Activación de usuarios de OpenManage Enterprise.....	139
Desactivación de usuarios de OpenManage Enterprise.....	139
Eliminación de usuarios de OpenManage Enterprise.....	139
Eliminación de servicios de directorio.....	139
Finalización de sesiones de usuario.....	140
Privilegios de usuario de OpenManage Enterprise basados en el rol.....	140
Adición y edición de usuarios de OpenManage Enterprise.....	141
Edición de propiedades de usuario de OpenManage Enterprise.....	142
Integración de servicios de directorio en OpenManage Enterprise.....	142
Importación de grupos de AD y LDAP.....	143
Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio.....	144
Adición o edición de grupos de LDAP que se utilizarán con los Servicios de directorio.....	144
Establecimiento de las propiedades de seguridad de inicio de sesión.....	145
Certificados de seguridad.....	146
Generación y descarga de la solicitud de firma de certificado.....	146
Asignar un certificado de servidor web a OpenManage Enterprise mediante los servicios de certificados de Microsoft.....	147
Administración de preferencias de consola.....	147
Personalizar la visualización de alertas.....	149
Administración de alertas entrantes.....	149
Configuración de credenciales de SNMP.....	150
Administración de la configuración de garantía.....	150
Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles.....	150

Actualizar los ajustes en OpenManage Enterprise.....	151
Actualizar OpenManage Enterprise.....	151
Actualización de Dell.com.....	152
Actualización de un recurso compartido de red interna.....	153
Instalar una extensión.....	154
Deshabilitar una extensión.....	155
Desinstalación de una extensión.....	155
Habilitación de una extensión.....	155
Ejecutar comandos y scripts remotos.....	155
Configuración de OpenManage Mobile.....	156
Activación o desactivación de notificaciones de alerta de OpenManage Mobile.....	157
Activación o desactivación de suscriptores de OpenManage Mobile.....	157
Eliminación de un suscriptor de OpenManage Mobile.....	158
Visualización del estado del servicio de notificación de alertas.....	158
Estado del servicio de notificación.....	158
Visualización de información acerca de los suscriptores de OpenManage Mobile.....	159
Información para suscriptores de OpenManage Mobile.....	159
Solución de problemas de OpenManage Mobile.....	160

Capítulo21: Otras descripciones de los campos y referencias.....161

Programar referencia.....	161
Definiciones de los campos de la línea base de firmware.....	161
Definiciones de los campos Programar trabajos.....	161
Categorías de alerta después de la reubicación de EEMI.....	162
Sustitución del token en secuencias de comandos remotas y política de alerta.....	163
Flujo de depuración de servicio de campo.....	163
Desbloquear la capacidad FSD.....	164
Instalar o conceder un archivo DAT.ini firmado de FSD.....	164
Llamar FSD.....	165
Desactivar FSD.....	165
Definiciones de campos de administración de catálogos.....	165
Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge.....	165

Lista de tablas

1. Otra información útil.....	12
2. Privilegios de usuario basados en roles en OpenManage Enterprise.....	15
3. Tipos de roles de usuario en OpenManage Enterprise.....	17
4. Requisitos mínimos recomendados de hardware.....	18
5. Requisitos mínimos.....	19
6. Parámetros que se usan en ovf_properties.config.....	23
7. Opciones de la interfaz de usuario de texto.....	26
8. Consideraciones de escalabilidad y rendimiento de OpenManage Enterprise.....	29
9. Protocolos y puertos admitidos por OpenManage Enterprise en estaciones de administración.....	29
10. Protocolos y puertos admitidos por OpenManage Enterprise en nodos administrados.....	31
11. Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise.....	32
12. Estados de los dispositivos en OpenManage Enterprise.....	39
13. Implementaciones compatibles entre plantillas.....	69
14. Tipos de red.....	77
15. Formato de definición VLAN para archivo CSV.....	79
16. Formato de definición de VLAN para archivos JSON.....	79
17. Administrar perfiles: definiciones de campos.....	80
18. Estados del perfil y operaciones posibles.....	80
19. Purga de alertas.....	95
20. Estado y descripción del trabajo.....	105
21. Tipos y descripción del trabajo.....	106
22. Matriz de compatibilidad de protocolos para detección.....	115
23. Privilegios de acceso basado en roles para administrar informes en OpenManage Enterprise.....	128
24. Privilegios de acceso basado en roles para generar informes en OpenManage Enterprise.....	131

25. Acceso basado en funciones para archivos de MIB en OpenManage Enterprise.....	133
26. Privilegios de usuario basados en roles en OpenManage Enterprise.....	140
27. Requisitos previos/atributos admitidos de OpenManage Enterprise para la integración de LDAP.....	142
28. Estado del servicio de notificación.....	158
29. Información para suscriptores de OpenManage Mobile.....	159
30. Solución de problemas de OpenManage Mobile.....	160
31. Categorías de alerta en OpenManage Enterprise.....	162
32. Tokens admitidos en OpenManage Enterprise.....	163
33. Convención de nomenclatura de servidores PowerEdge junto con ejemplos.....	166

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:

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

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

- Acceso basado en funciones que limita el acceso a las configuraciones de la consola y a las acciones del dispositivo.
- 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 (HTTPS).
- 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](#) en la página 18
- [Configurar OpenManage Enterprise con interfaz de usuario de texto](#) en la página 25
- [Detección de dispositivos para la supervisión o administración](#) en la página 110
- [Administración de dispositivos](#) en la página 40
- [Supervisión de dispositivos mediante el tablero de OpenManage Enterprise](#) en la página 35
- [Organizar los dispositivos en grupos](#) en la página 36
- [Administrar el firmware y los controladores del dispositivo](#) en la página 55
- [Visualización y configuración de dispositivos](#) en la página 50
- [Supervisión de alertas de dispositivos](#) en la página 93
- [Visualizar las alertas archivadas](#) en la página 95
- [Ver y renovar la garantía del dispositivo](#) en la página 126
- [Administrar las plantillas de configuración de dispositivos](#) en la página 64
- [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86
- [Administrar plantillas de línea base de cumplimiento](#) en la página 87
- [Administrar registros de auditoría](#) en la página 103
- [Administración de los ajustes del servidor OpenManage Enterprise](#) en la página 136
- [Ejecución de un trabajo de inventario ahora](#) en la página 124

- [Administración de la garantía del dispositivo](#) en la página 126
- [Informes](#) en la página 128
- [Administración de archivos de MIB](#) en la página 133
- [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
- [Integración de servicios de directorio en OpenManage Enterprise](#) en la página 142

Temas:

- [Novedades de esta versión](#)
- [Otra información útil](#)
- [Cómo ponerse en contacto con Dell EMC](#)
- [Licencia de OpenManage Enterprise Advanced](#)

Novedades de esta versión

- Detección iniciada por servidor: con esta función, los nuevos servidores en un centro de datos pueden notificar a OpenManage Enterprise y se pueden descubrir automáticamente. Los servidores deben tener una versión de firmware de 4.00.00.00 o posterior.
- Administración de la configuración mediante perfiles: esta función permite la creación previa de perfiles con una configuración específica de dispositivo (incluidas las identidades virtuales) para su posterior implementación en dispositivos. La administración de perfiles permite una migración fácil de la configuración de un dispositivo a otro.
- Compatibilidad de actualización de controladores en banda para los dispositivos que se ejecutan en versiones de Windows de 64 bits.
- Los atributos de identidad no virtual pueden heredar valores desde la plantilla de origen y editarse antes de su implementación o su implementación automática.
- Se pueden editar los atributos de seguridad de las plantillas, por ejemplo, las contraseñas.
- Identifique y marque las identidades “asignadas” en el inventario de configuración del dispositivo.
- Se incluye un informe preestablecido de “Uso de identidad virtual por grupo” en la sección Informes.
- Mejoras:
 - Los cambios en la configuración de VLAN en las plantillas se pueden propagar inmediatamente en sistemas modulares.
 - Compatibilidad con las plataformas YX4X XC (14G XC). Para obtener más información, consulte la matriz de soporte de OpenManage Enterprise versión 3.4.
 - Asignación mejorada de identidades virtuales: las identidades virtuales que no están asignadas desde OpenManage Enterprise se identifican automáticamente y se marcan como “asignadas”.
 - Mejora en la solidez y el escalamiento para el inventario de configuración del servidor.
 - En caso de que se produzca una falla en la actualización de consola, se restaurará el estado preinstalado del dispositivo.

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
<i>Matriz de compatibilidad de Dell EMC OpenManage Enterprise</i>	Permite ver los dispositivos compatibles con OpenManage Enterprise.	<ol style="list-style-type: none"> 1. Vaya a Dell.com/OpenManageManuals. 2. Haga clic en OpenManage Enterprise y seleccione la versión requerida de OpenManage Enterprise. 3. Haga clic en Documentación para tener acceso a estos documentos.
<i>Notas de la versión Dell EMC OpenManage Enterprise</i>	Permite obtener información sobre problemas conocidos y soluciones alternativas en OpenManage Enterprise.	
<i>Guía del usuario de Dell EMC OpenManage Mobile</i>	Proporciona información acerca de la instalación y el uso de la aplicación OpenManage Mobile.	
<i>Guía del usuario de administrador de repositorios de Dell EMC</i>	Proporciona información sobre el uso de Repository Manager para administrar las actualizaciones del sistema.	
<i>Guía de API RESTful de OpenManage Enterprise y</i>	Permite obtener información sobre la integración de OpenManage Enterprise mediante las API de	

Tabla 1. Otra información útil (continuación)

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

Cómo ponerse en contacto con Dell EMC

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

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

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

Licencia de OpenManage Enterprise Advanced

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

La licencia de *OpenManage Enterprise Advanced* es perpetua y válida durante toda la vida útil del servidor; además, puede vincularse con la etiqueta de servicio de solo un servidor a la vez. OpenManage Enterprise ofrece un informe integrado para ver la lista de dispositivos y sus licencias. Seleccione **OpenManage Enterprise > Supervisión > Informes > Informe de licencia** y luego haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

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

Licencia OpenManage Enterprise Advanced, servidores compatibles

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

- Servidores YX3X que tienen las versiones de firmware 2.50.50.50 de iDRAC8 o posteriores. Las versiones de firmware de YX3X son compatibles con versiones anteriores y se pueden instalar en un hardware de YX2X. Consulte [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165.
- Servidores YX4X que tienen las versiones de firmware 3.10.10.10 de iDRAC9 o posteriores. Consulte [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165

Adquirir la licencia de OpenManage Enterprise Advanced

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

Verificación de la información de la licencia

OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos que supervisa OpenManage Enterprise y sus licencias. Haga clic en **OpenManage Enterprise > Supervisión > Informes > Informe de la licencia**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

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

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

Funciones basadas en la licencia en OpenManage Enterprise

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

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

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

Características de seguridad en OpenManage Enterprise

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

- Funciones del usuario (administrador, administrador de dispositivos, observador) con diferente funcionalidad de administración de dispositivos.
- Servidor reforzado con Security-Enhanced Linux (SELinux) y un firewall interno.
- Cifrado de datos confidenciales en una base de datos interna.
- Uso de comunicación cifrada fuera del dispositivo (HTTPS).

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

NOTA:

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

Información relacionada

[Implementación y administración de OpenManage Enterprise](#) en la página 18

Temas:

- [Privilegios de usuario de OpenManage Enterprise basados en el rol](#)
- [Tipos de roles de usuario en 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. Esta función se conoce como Control de acceso basado en funciones (RBAC). La consola se aplica a una de las funciones por cuenta. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte [Administración de usuarios de OpenManage Enterprise](#) en la página 138.

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

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

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Admin (Administrador)	Administrador de dispositivos	Observador
Ejecutar informes	S	S	S

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

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Admin (Administrador)	Administrador de dispositivos	Observador
Ver	S	S	S
Administrar plantillas	S	S	N
Administrar perfiles	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 sistemas operativos	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
Seleccionar destinos para la implementación automática	S	N	N

Referencias relacionadas

[Tipos de roles de usuario en OpenManage Enterprise](#) en la página 16

Tareas relacionadas

[Implementación y administración de OpenManage Enterprise](#) en la página 18

Tipos de roles de usuario en OpenManage Enterprise

NOTA:

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

Tabla 3. Tipos de roles de usuario en OpenManage Enterprise

El usuario con este rol...	Tiene los siguientes privilegios del usuario
Administrador	<p>Tiene acceso completo a todas las tareas que se pueden realizar en la consola.</p> <ul style="list-style-type: none"> • Acceso total (mediante GUI y REST) para leer, ver, crear, editar, eliminar, exportar y quitar información relacionada con los dispositivos y grupos que supervisa OpenManage Enterprise. • Puede crear usuarios de Microsoft Active Directory (AD), de LDAP y locales, y asignar roles adecuados • Activar y desactivar usuarios • Modificar los roles de los usuarios existentes • Eliminar los usuarios • Cambiar la contraseña de usuario
Administrador de dispositivos (DM)	<ul style="list-style-type: none"> • Ejecute tareas, políticas y otras acciones en los dispositivos asignados por el administrador. • No puede eliminar ni modificar grupos. <p>NOTA: No se pueden asignar grupos a los usuarios con privilegios de administrador de dispositivos (DM).</p>
Observador	<ul style="list-style-type: none"> • Solo puede ver la información que se muestra en OpenManage Enterprise y ejecutar informes. • De manera predeterminada, tiene acceso de solo lectura a la consola y todos los grupos. • No se puede ejecutar las tareas ni crear y administrar políticas.

NOTA:

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

Tareas relacionadas

[Implementación y administración de OpenManage Enterprise](#) en la página 18

Información relacionada

[Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15

Implementación y administración de OpenManage Enterprise

Dell EMC OpenManage Enterprise se proporciona como un servidor que puede implementarse en un hipervisor y permite administrar recursos para minimizar el tiempo de inactividad. El servidor virtual se puede configurar desde la consola web de aplicaciones después del aprovisionamiento inicial de la red en la interfaz de usuario de texto (TUI). Para conocer los pasos para ver y actualizar la versión de la consola, consulte [Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles](#) en la página 150. En este capítulo se describen los requisitos previos y mínimos para la instalación.

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

Referencias relacionadas

[Tipos de roles de usuario en OpenManage Enterprise](#) en la página 16

[Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise](#) en la página 33

[Características de seguridad en OpenManage Enterprise](#) en la página 15

Información relacionada

[Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15

Temas:

- [Prerrequisitos de instalación y requisitos mínimos](#)
- [Implementar OpenManage Enterprise en VMware vSphere](#)
- [Implementar OpenManage Enterprise en Hyper-V 2012 R2 y host anteriores](#)
- [Implementar OpenManage Enterprise en un host de Hyper-V 2016](#)
- [Implementar OpenManage Enterprise en un host de Hyper-V 2019](#)
- [Implementación de OpenManage Enterprise utilizando una máquina virtual basada en kernel](#)
- [Implementar mediante programación OpenManage Enterprise](#)

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	32 GB	16 GB
Procesadores	8 núcleos en total	4 núcleos en total

Tabla 4. Requisitos mínimos recomendados de hardware (continuación)

Requisitos mínimos recomendados de hardware	Implementaciones amplias	Implementaciones pequeñas
Unidad de disco duro	250 GB	50 GB

Requisitos mínimos del sistema para implementar OpenManage Enterprise

Tabla 5. Requisitos mínimos

Detalles	Requisitos mínimos
Hipervisores compatibles	<ul style="list-style-type: none"> · Versiones de VMware vSphere: <ul style="list-style-type: none"> ○ vSphere ESXi 5.5 en adelante · Microsoft Hyper-V compatible en: <ul style="list-style-type: none"> ○ Windows Server 2012 R2 en adelante · KVM compatible en: <ul style="list-style-type: none"> ○ Red Hat Enterprise Linux 6.5 en adelante
Red	NIC virtual disponible que tiene acceso a las redes de administración de todos los dispositivos administrados desde OpenManage Enterprise.
Navegadores compatibles	<ul style="list-style-type: none"> · Internet Explorer (64 bits) 11 y versiones posteriores · Mozilla Firefox 52 y versiones posteriores · Google Chrome 58 y versiones posteriores · Microsoft Edge versión 41.16299 y versiones posteriores
Interfaz de usuario	HTML 5, basado en JS

NOTA: Para ver la actualización más reciente de los requisitos mínimos para OpenManage Enterprise, consulte *Matriz de soporte de Dell EMC OpenManage Enterprise* 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](#) en la página 15.

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

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


7. En función de la configuración de vCenter, aparecerá una de las siguientes opciones:
 - **Si se han configurado bloques de recursos:** en la página **Bloque de recursos**, seleccione el bloque de dispositivos virtuales para implementar la aplicación VM.
 - **Si NO se han configurado bloques de recursos:** en la página **Hosts o clústeres**, seleccione el host o el clúster en el que desea implementar la máquina virtual del dispositivo.
8. Si hay más de un almacén de datos disponible en el host, en la página **Almacén de datos** se muestran esos almacenes de datos. Seleccione la ubicación para almacenar los archivos de máquinas virtuales (VM) y, a continuación, haga clic en **Siguiente**.
9. En la página **Formato de disco**, haga clic en **Aprovisionamiento grueso** para preasignar espacio físico de almacenamiento a máquinas virtuales en el momento en que se crea una unidad.
10. En la página **Listo para completar**, revise las opciones que seleccionó en las páginas anteriores y haga clic en **Finalizar** para ejecutar el trabajo de implementación.


De este modo, se muestra una ventana del estado de finalización donde puede realizar un seguimiento del trabajo de detección.


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


NOTA:


- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
 - Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como DESHABILITADO y el usuario deberá configurarlo.
 - Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.
1. Descargue el archivo `openmanage_enterprise_vhd_format.zip` desde el sitio de soporte. Extraiga el archivo y, a continuación, mueva o copie el archivo VHD adjunto a la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
 2. Inicie el **Administrador de Hyper-V** en Windows Server 2012 R2 o en una versión anterior. Windows Hyper-V debe aparecer en el administrador de Hyper-V. Si no es así, haga clic con el botón secundario en **Administrador de Hyper-V** y seleccione **Conectar al servidor**.
 3. Haga clic en **Acciones > Nueva > Máquina virtual** para iniciar el **Asistente de nueva máquina virtual**.
 4. Haga clic en **Siguiente** en la página inicial **Antes de comenzar**.
 5. En la **página Especificar nombre y ubicación**,
 - proporcione el **Nombre de la máquina virtual**.
 - (Opcional) Seleccione la casilla de verificación **Almacenar la máquina virtual en una ubicación diferente** para activar el campo **Ubicación** y, a continuación, navegue para capturar una ubicación de la carpeta en la que se almacena la VM.

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

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

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

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

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

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

Implementar OpenManage Enterprise en un host de Hyper-V 2016


NOTA:


- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como DESHABILITADO y el usuario deberá configurarlo.
- Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.


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


 **NOTA:** Si no está seleccionada la casilla de verificación, la máquina virtual se almacena en la carpeta predeterminada.

6. Haga clic en **Siguiente**.
7. En la página **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.

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

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

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

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

Implementar OpenManage Enterprise en un host de Hyper-V 2019

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15

- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como DESHABILITADO y el usuario deberá configurarlo.
- Después de instalar o actualizar el dispositivo en Hyper-V, apague el dispositivo, quite el adaptador de red estándar y agregue un adaptador de red heredado; luego, encienda el dispositivo.

1. Descargue el archivo **openmanage_enterprise_vhd_format.zip** desde el sitio de soporte. Extraiga el archivo y, a continuación, mueva o copie el archivo VHD adjunto a la ubicación adecuada del sistema en el que desee almacenar la unidad virtual OpenManage Enterprise.
 2. Inicie el **Administrador de Hyper-V** en Windows Server 2019. Windows Hyper-V debe aparecer en el administrador de Hyper-V. Si no es así, haga clic con el botón secundario en **Administrador de Hyper-V** y seleccione **Conectar al servidor**.
 3. Haga clic en **Acciones > Nueva > Máquina virtual** para iniciar el **Asistente de nueva máquina virtual**.
 4. Haga clic en **Siguiente** en la página inicial **Antes de comenzar**.
 5. En la **página Especificar nombre y ubicación**,
 - proporcione el **Nombre de la máquina virtual**.
 - (Opcional) Seleccione la casilla de verificación **Almacenar la máquina virtual en una ubicación diferente** para activar el campo **Ubicación** y, a continuación, navegue para capturar una ubicación de la carpeta en la que se almacena la VM.
- NOTA:** Si no está seleccionada la casilla de verificación, la máquina virtual se almacena en la carpeta predeterminada.
6. Haga clic en **Siguiente**.
 7. En la página **Especificar generación**, seleccione **Generación 1** y, a continuación, haga clic en **Siguiente**.
- NOTA:** OpenManage Enterprise no es compatible con la 2.ª generación.
8. En la página **Asignar memoria**, ingrese la memoria de inicio en el campo **Memoria de inicio** y haga clic en **Siguiente**.
- NOTA:** Asegúrese de que se asigne un mínimo de 16 000 MB (16 GB).
9. En la página **Configurar redes**, seleccione el adaptador de red en la lista desplegable **Conexión**. Asegúrese de que el **Switch virtual** esté conectado a la red. Haga clic en **Siguiente**.
- NOTA:** Si se establece en "No Conectado", OME no funcionará correctamente durante el primer reinicio y es necesario implementarlo nuevamente, si vuelve a ocurrir esta situación.
10. En la página **Conectar disco duro virtual**, seleccione **Usar una unidad de disco virtual existente** y, a continuación, navegue a la ubicación en la que se copió el archivo VHD como se indica en el **paso 1**. Haga clic en **Siguiente**.
 11. Complete las instrucciones que aparecen en pantalla.
- NOTA:** Asegúrese de tener un tamaño de almacenamiento mínimo de 20 GB
12. Abra la **Configuración** de la nueva MV creada y encienda la VM.
 13. En la pantalla TUI, acepte el EULA y, cuando se le indique, cambie la contraseña del dispositivo y establezca los parámetros de red para la IP del dispositivo.

Implementación de OpenManage Enterprise utilizando una máquina virtual basada en kernel

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
- Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como DESHABILITADO y el usuario deberá configurarlo.

1. Instale los paquetes de virtualización requeridos mientras instala el sistema operativo.
2. Descargue el archivo **openmanage_enterprise_kvm_format.zip** desde el sitio de soporte. Descargue el archivo en la ubicación correspondiente del sistema en la que desee almacenar la unidad virtual OpenManage Enterprise.
3. Inicie el administrador virtual y seleccione **Archivo > Propiedades**.
4. En la página **Interfaces de red**, haga clic en **Agregar**.
5. Seleccione **Puente** como tipo de interfaz y haga clic en **Reenviar**.
6. Configure el modo de inicio como **en arranque** y seleccione la casilla de verificación **Activar ahora**.

7. Seleccione la interfaz que va a conectar desde la lista, asegúrese de que las propiedades coinciden con el dispositivo de host y, luego, haga clic en **Finalizar**.
Se acaba de crear una interfaz virtual y puede configurar la configuración del firewall usando el terminal.
8. En el administrador de máquina virtual, haga clic en **Archivo > Nuevo**.
9. Ingrese un nombre para la máquina virtual, seleccione la opción **Importar imagen de disco existente** y haga clic en **Reenviar**.
10. Vaya al sistema de archivos y seleccione el archivo QCOW2 que se descargó en el paso 1. Luego, haga clic en **Reenviar**.
11. Asigne 16 GB como la memoria y seleccione dos núcleos de procesador. A continuación, haga clic en **Reenviar**.
12. Asigne el espacio en disco necesario para la máquina virtual y haga clic en **Reenviar**.
13. En **Opciones avanzadas**, asegúrese de que la red del dispositivo host con puente está seleccionada y de que el Tipo de virtualización seleccionado sea KVM.
14. Haga clic en **Finalizar**.
El dispositivo OpenManage Enterprise ya está implementado usando el KVM. Para comenzar a utilizar OpenManage Enterprise, consulte [Iniciar sesión en OpenManage Enterprise](#) en la página 25.

Implementar mediante programación OpenManage Enterprise

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

- NOTA:** La implementación programática o con script solo es compatible mediante el uso de la interfaz principal.
- NOTA:** Si se agrega un adaptador secundario antes de encender el dispositivo por primera vez, el adaptador se configurará con IPv4 e IPv6 deshabilitados. Tras iniciar sesión en la TUI y después de aceptar el EULA y cambiar la contraseña de administrador, el adaptador se mostrará como DESHABILITADO y el usuario deberá configurarlo.
- NOTA:** Para la implementación programática, debe utilizar las versiones más recientes de la Herramienta OVF y Python 3.0 o posteriores.

Para implementar mediante programación OpenManage Enterprise, realice lo siguiente:

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

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

Parámetro	Valores aceptables	Descripción
<code>bEULATxt</code>	verdadero o falso	Si configura este valor como verdadero, acepta los términos y condiciones del acuerdo de licencia del usuario final (EULA). El EULA está disponible al final del archivo <code>ovf_properties.config</code> .
<code>adminPassword</code>	Debe contener al menos un carácter en: mayúscula, minúscula, dígito y carácter especial. Por ejemplo, Dell123\$	Escriba una nueva contraseña de administrador para OpenManage Enterprise.
<code>bEnableDHCP</code>	verdadero o falso	Establezca como verdadero, si desea que el dispositivo habilite IPv4 DHCP y para omitir la IPv4 estática.
<code>bEnableIpv6AutoConfig</code>	verdadero o falso	Configure como verdadero, si desea que el dispositivo habilite la configuración

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

Parámetro	Valores aceptables	Descripción
		automática de IPv6 y para omitir la IPv6 estática.
<code>staticIP</code>	IP estática en formato CIDR	Puede ser IPv4 o IPv6. (No puede configurar al mismo tiempo los tipos IPv4 e IPv6).
<code>gateway</code>	IPv4 o IPv6	No puede configurar al mismo tiempo la puerta de enlace estática como tipos IPv4 e IPv6.

3. Ejecute el script `update_ovf_property.py`.

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

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

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

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

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

Introducción a OpenManage Enterprise

Temas:

- Iniciar sesión en OpenManage Enterprise
- Configurar OpenManage Enterprise con interfaz de usuario de texto
- Configurar OpenManage Enterprise
- Configuración recomendada de escalabilidad y rendimiento para el uso óptimo de OpenManage Enterprise
- Protocolos y puertos admitidos en OpenManage Enterprise
- Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise

Iniciar sesión en OpenManage Enterprise

Cuando se inicia el sistema por primera vez en la interfaz de usuario de texto (TUI), se le pedirá que acepte el EULA y, a continuación, que cambie la contraseña del administrador. Si iniciará sesión en OpenManage Enterprise por primera vez, debe establecer las credenciales de usuario a través de la TUI. Consulte [Configurar OpenManage Enterprise con interfaz de usuario de texto](#) en la página 25.

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

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

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

Si está iniciando sesión en OpenManage Enterprise por primera vez, aparece la página **Bienvenido a OpenManage Enterprise**. Haga clic en **Configuración inicial** y complete la configuración básica. Consulte [Configurar OpenManage Enterprise](#) en la página 28. Para detectar los dispositivos, haga clic en **Detectar dispositivos**.

NOTA: De manera predeterminada, después de tres intentos de inicio de sesión fallidos, la cuenta de OpenManage Enterprise se bloquea y no puede iniciar sesión hasta que finalice la duración del bloqueo de cuenta. La duración del bloqueo de cuenta es de 900 segundos de forma predeterminada. Para cambiar este período, consulte [Establecimiento de las propiedades de seguridad de inicio de sesión](#) en la página 145.

Configurar OpenManage Enterprise con interfaz de usuario de texto

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

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

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

NOTA:

- Para configurar IPv6, asegúrese de que ya esté configurado por un vCenter Server.
- De manera predeterminada, OpenManage Enterprise utiliza la última IP detectada de un dispositivo para realizar todas las operaciones. Para aplicar cualquier cambio de IP, es necesario volver a detectar el dispositivo.

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

Tabla 7. Opciones de la interfaz de usuario de texto

Opciones	Descripciones
Cambiar la contraseña del administrador	<p>Seleccione la pantalla Cambiar la contraseña del administrador para ingresar una nueva contraseña y confírmela.</p> <p>La primera vez, debe cambiar la contraseña en la pantalla TUI.</p>
Ver estado del dispositivo actual	<p>Seleccione Mostrar estado actual del dispositivo para ver la dirección URL y el estado del dispositivo. También puede ver los estados de la ejecución de tareas, el procesamiento de eventos, Tomcat, la base de datos y los servicios de supervisión.</p>
Ver la configuración de red actual	<p>Seleccione Mostrar la configuración de red actual para ver los detalles de la configuración de IP.</p> <p>En el menú Elegir adaptador de red, se enumeran todos los adaptadores de red disponibles. Si hace clic en un adaptador de red, se mostrará su configuración actual.</p>
Establecer parámetros del sistema de red	<p>Seleccione Establecer parámetros de red para volver a configurar los adaptadores de red.</p> <p>En el menú Elegir adaptador de red, se enumeran todos los adaptadores de red disponibles. Seleccione un adaptador de red, vuelva a configurar los parámetros de red y seleccione Aplicar para guardar los cambios en la interfaz correspondiente.</p> <p>De forma predeterminada, solo IPv4 está habilitada en la interfaz de red principal con una IP estática privada en el dispositivo. Sin embargo, si se agrega una nueva interfaz de red, tanto IPv4 como IPv6 estarán habilitadas para el alojamiento múltiple.</p> <p>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.</p> <p>NOTA:</p> <ul style="list-style-type: none"> • La configuración DNS solo está disponible en la interfaz de red principal. Si se desea la resolución del DNS en esta interfaz, se deben poder resolver todos los nombres de host mediante el servidor DNS configurado en la interfaz principal.
Seleccionar interfaz de red principal	<p>Seleccionar interfaz de red principal le permite designar una red principal.</p> <p>La selección de una interfaz principal otorga prioridad a la interfaz seleccionada en términos de enrutamiento y se utiliza como la ruta predeterminada. Esta interfaz tendrá la prioridad de enrutamiento en caso de cualquier ambigüedad. También se espera que la interfaz principal sea la interfaz "pública" que habilita la conexión a Internet o la red corporativa. Se aplican diferentes reglas de firewall a la interfaz principal, lo que permite un control de acceso más estricto, como la restricción de acceso por rango de IP.</p> <p>NOTA: Si el alojamiento múltiple está habilitado, se puede acceder al dispositivo desde dos redes. En este caso, el dispositivo utiliza la interfaz principal para toda la comunicación externa y cuando se utiliza la configuración del proxy. Para obtener más información</p>

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

Opciones	Descripciones
	<p>sobre el alojamiento múltiple en OpenManage, consulte la documentación técnica sobre la <i>Ejecución de scripts remotos con Dell EMC OpenManage Enterprise</i> en el sitio de soporte.</p>
Configurar rutas estáticas	<p>Seleccione Configurar rutas estáticas si las redes requieren la configuración de una ruta estática para comunicarse con una subred específica a través de las redes IPv4 e IPv6.</p> <p>NOTA: Se admite un máximo de 20 rutas estáticas por interfaz.</p>
Configurar detección iniciada por servidor	<p>Seleccione Configurar detección iniciada por servidor para permitir que el dispositivo genere de manera automática los registros necesarios con el servidor DNS configurado.</p> <p>NOTA:</p> <ul style="list-style-type: none"> • Asegúrese de que el dispositivo esté registrado en DNS y que pueda actualizar de forma dinámica los registros. • Los sistemas de destino deben estar configurados para solicitar los detalles de registro de DNS. • Para cambiar el nombre de dominio de DNS, asegúrese de que el registro de DNS dinámico esté activado en el servidor DNS. Además, registrar el dispositivo en el servidor DNS, seleccione la opción Seguros y no seguros en Actualizaciones dinámicas.
Activar modo Depuración de servicio de campo (FSD)	<p>Seleccione Activar modo de depuración de servicio de campo (FSD) para la depuración de la consola. Para obtener más información, consulte Flujo de depuración de servicio de campo en la página 163.</p>
Reiniciar servicios	<p>Seleccione Reiniciar servicios con las siguientes opciones para reiniciar los servicios y las redes:</p> <ul style="list-style-type: none"> • Reiniciar todos los servicios • Reiniciar la red
Configurar registro de depuración	<p>Seleccione Configurar registro de depuración utilizando las siguientes opciones:</p> <ul style="list-style-type: none"> • Activar registros de depuración: se utiliza para recolectar los registros de depuración de las tareas de supervisión de la aplicación, los eventos y el historial de ejecución de tareas. • Desactivar registros de depuración: se utiliza para desactivar los registros de depuración. • Activar retención de SCP: se utiliza para recolectar los archivos .XML de la plantilla. • Desactivar retención de SCP: se utiliza para desactivar la retención de SCP. <p>Puede descargar los registros de depuración haciendo clic en Supervisión > Registros de auditoría > Exportar > Exportar registros de consola en OpenManage Enterprise.</p>
Cambiar el diseño del teclado	<p>Seleccione Cambiar la distribución del teclado para cambiar la distribución del teclado si es necesario.</p>
Reiniciar el dispositivo	<p>Seleccione Reiniciar el dispositivo para reiniciar el dispositivo.</p> <p>NOTA: Después de ejecutar un comando para reiniciar los servicios, es posible que la TUI muestre el siguiente</p>

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

Opciones	Descripciones
	<p><code>mensaje: NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439].</code></p> <p>El problema de bloqueo parcial probablemente se produce como resultado de la sobrecarga del hipervisor. En dichas situaciones, se recomienda tener al menos 16 GB de RAM y una CPU de 8000 MHz reservada para el dispositivo OpenManage Enterprise. Además, se recomienda reiniciar el dispositivo OpenManage Enterprise cuando aparezca este mensaje.</p>

Configurar OpenManage Enterprise

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

1. Para configurar manualmente la hora, realice lo siguiente en la sección **Configuración de hora**:

- Utilice el menú desplegable **Zona horaria** para seleccionar la zona horaria correspondiente.
- En el cuadro **Fecha**, ingrese o seleccione una fecha.
- En el cuadro **Hora**, complete la hora.
- Haga clic en **Aplicar** para guardar la configuración.

2. Si desea utilizar el servidor NTP para sincronizar la hora, haga lo siguiente en la sección **Configuración de hora**:

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

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

3. Si desea establecer el servidor proxy para comunicación externa, en la sección Configuración del proxy, haga lo siguiente:

- Seleccione la casilla de verificación **Habilitar configuración de proxy HTTP**.
- Ingrese la **Dirección proxy**.
- Ingrese el **Número del puerto** para el servidor proxy.
- Si el servidor proxy requiere credenciales para iniciar sesión, seleccione la casilla de verificación **Habilitar autenticación de proxy** y, a continuación, ingrese el nombre de usuario y la contraseña.
- Seleccione la casilla de verificación **Ignorar validación del certificado** si el proxy configurado intercepta el tráfico SSL y no usa ningún certificado de confianza de otros fabricantes. Si se usa esta opción, se omitirán las comprobaciones incorporadas del certificado, que se utilizan para la sincronización de la garantía y el catálogo.

4. Haga clic en **Aplicar** para guardar la configuración.

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

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

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

Tabla 8. Consideraciones de escalabilidad y rendimiento de OpenManage Enterprise

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

Protocolos y puertos admitidos en OpenManage Enterprise

Protocolos y puertos admitidos en Management Stations

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

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
22	SSH	TCP	256 bits	Estación de administración	Entrada	Dispositivo OpenManage Enterprise	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Para recibir alertas de OpenManage Enterprise por correo electrónico.
53	DNS	UDP/TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	<ul style="list-style-type: none"> Para realizar consultas DNS.
68/546 (IPv6)	DHCP	UDP/TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	<ul style="list-style-type: none"> Configuración de red.

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

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
80*	HTTP	TCP	Ninguno	Estación de administración	Entrada	Dispositivo OpenManage Enterprise	<ul style="list-style-type: none"> La página principal de la interfaz gráfica de usuario web. Esto redirigirá a un usuario a HTTPS (puerto 443).
123	NTP	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Servidor NTP	<ul style="list-style-type: none"> Sincronización de hora (si está activada).
137, 138, 139, 445	CIFS	UDP/TCP	Ninguno	IDRAC/CMC	Entrada	Dispositivo OpenManage Enterprise	<ul style="list-style-type: none"> Para cargar o descargar plantillas de configuración de dispositivos. Para cargar TSR y los registros de diagnóstico. Para descargar los DUP de firmware/controlador y el proceso FSD. Arrancar en el ISO de red.
				Dispositivo OpenManage Enterprise	Salida	Recurso compartido de CIFS	<ul style="list-style-type: none"> Para importar catálogos de firmware o controladores desde el recurso compartido CIFS.
162*	SNMP	UDP	Ninguno	Estación de administración	Entrada/Salida	Dispositivo OpenManage Enterprise	<ul style="list-style-type: none"> Recepción de sucesos mediante SNMP. La dirección es de 'salida' solo si se utiliza la política de reenvío de captura.
443 (valor predeterminado)	HTTPS	TCP	SSL de 128 bits	Estación de administración	Entrada/Salida	Dispositivo OpenManage Enterprise	<ul style="list-style-type: none"> 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.

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

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
							<ul style="list-style-type: none"> Detección iniciada por servidor.
514	Syslog	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Servidor Syslog	<ul style="list-style-type: none"> Para enviar un alerta e información de registros de auditoría al servidor Syslog.
3269	LDAPS	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	<ul style="list-style-type: none"> Inicio de sesión AD/LDAP para catálogo global.
636	LDAPS	TCP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Estación de administración	<ul style="list-style-type: none"> Inicio de sesión AD/LDAP para controlador de dominio.

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

Protocolos y puertos admitidos en nodos administrados

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

Número de puerto	Protocolo	Tipo de puerto	Nivel de cifrado máximo	Origen	Dirección	Destination	Uso
22	SSH	TCP	256 bits	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	<ul style="list-style-type: none"> Para la detección de Hyper-V, Linux OS y Windows.
161	SNMP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	<ul style="list-style-type: none"> Para hacer consultas SNMP.
162*	SNMP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Entrada/Salida	Nodo administrado	<ul style="list-style-type: none"> Enviar y recibir capturas de SNMP
443	Propio/W S-Man/ Redfish	TCP	256 bits	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	<ul style="list-style-type: none"> Detección e inventario de iDRAC7 y versiones posteriores. Para la administración de CMC.
623	IPMI/RMCP	UDP	Ninguno	Dispositivo OpenManage Enterprise	Salida	Nodo administrado	<ul style="list-style-type: none"> Acceso a IPMI mediante LAN
69	TFTP	UDP	Ninguno	CMC	Entrada	Estación de administración	<ul style="list-style-type: none"> Para actualizar el firmware de CMC.

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

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

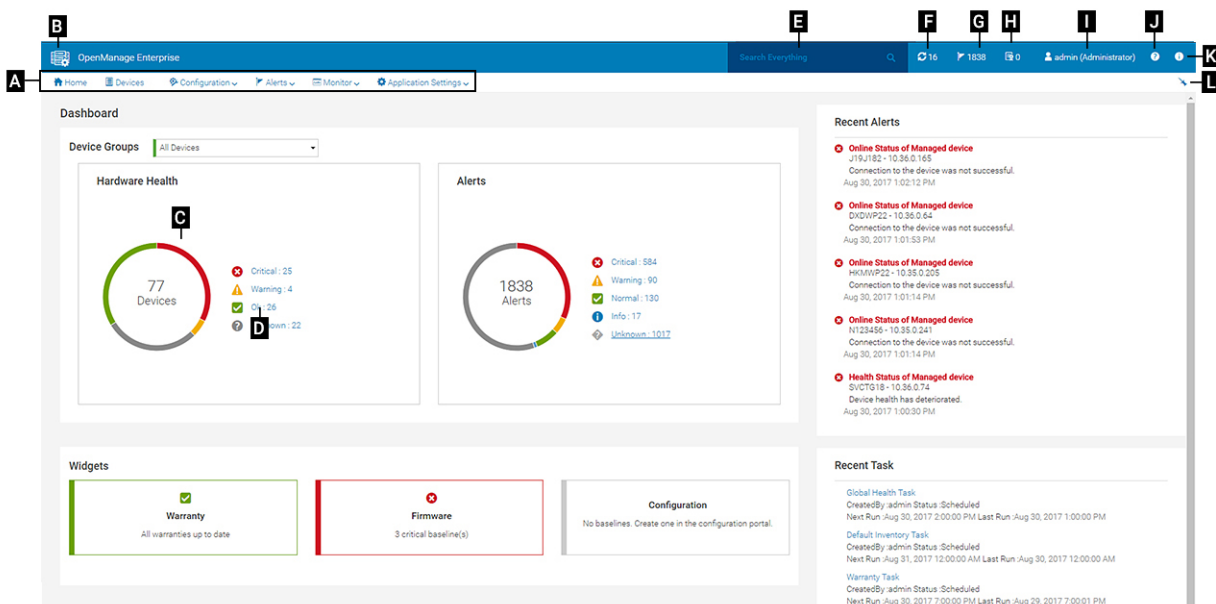
Vínculos de caso de uso para los protocolos y puertos admitidos en OpenManage Enterprise

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

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

Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise

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



- A: el menú **OpenManage Enterprise** en todas las páginas de OpenManage Enterprise proporciona enlaces a las características que permiten a los administradores ver el panel (**Inicio**), administrar los dispositivos (**Dispositivos**), administrar las bases del firmware y los controladores, las plantillas y las bases de cumplimiento de la configuración (**Configuración**), crear y almacenar las alertas (**Alertas**) y, luego, ejecutar trabajos, detectar, recolectar datos de inventario y generar informes (**Supervisión**). También puede personalizar las diversas propiedades de OpenManage Enterprise (**Configuración de la aplicación**). Haga clic en el símbolo de alfiler en la esquina superior derecha para fijar los elementos de menú, de modo que aparezcan en todas las páginas de OpenManage Enterprise. Para quitarlos, nuevamente haga clic en el símbolo de alfiler.
- B: Símbolo del Panel. Haga clic en este símbolo para abrir la página de panel en cualquier página de OpenManage Enterprise. De manera alternativa, haga clic en **Inicio**. Consulte [Panel](#).
- C: el gráfico de anillo proporciona una instantánea del estado de todos los dispositivos supervisados por OpenManage Enterprise. Le permite tomar acciones rápidamente con aquellos dispositivos que se encuentran en estado crítico. Cada color en el gráfico representa un grupo de dispositivos que tienen un estado de condición en particular. Haga clic en las respectivas bandas de colores para ver los dispositivos correspondientes en la lista de dispositivos. Haga clic en el nombre del dispositivo o en una dirección IP para ver la página de propiedades del dispositivo. Consulte [Visualización y configuración de dispositivos](#) en la página 50.
- D: Los símbolos utilizados para indicar el estado de los dispositivos. Consulte [Estados de los dispositivos](#) en la página 39.
- E: en el cuadro **Buscar todo**, ingrese lo que esté sujeto a monitoreo y que se pueda mostrar en OpenManage Enterprise para ver los resultados como la dirección IP del dispositivo, el nombre del trabajo, el nombre del grupo, la base del firmware o los controladores 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 "**

- F: número de trabajos de OpenManage Enterprise que actualmente se encuentran en la línea de espera. Trabajos relacionados con la detección, el inventario, la garantía y la actualización del firmware o los dispositivos, entre otros. Haga clic para ver el estado de los trabajos que se ejecutan bajo las categorías de Estado, Inventario e Informe en la página Detalles del trabajo. Para ver todos los eventos, haga clic en **Todos los trabajos**. Consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105. Haga clic en Actualizar.
- G: número de eventos generados en los registros de alerta. Además, la cantidad de alertas en esta sección varía en función de la configuración para ver o no las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Para ocultar o mostrar la alertas confirmadas, consulte [Personalizar la visualización de alertas](#) en la página 149. La eliminación de las alertas reduce la cuenta. Para obtener más información sobre los símbolos que se usan para indicar los estados de gravedad, consulte [Estados de los dispositivos](#) en la página 39. Haga clic en un símbolo de gravedad para ver todos los eventos en esa categoría de gravedad en la página Alertas. Para ver todos los servicios, haga clic en **Todos los eventos**. Consulte [Administración de alertas de dispositivos](#).
- H: cantidad total de garantías de dispositivos en estados críticos (vencidas) y de advertencia (que caducan pronto). Consulte [Administración de garantía de dispositivos](#).
- I: nombre del usuario actualmente conectado. Detenga el puntero sobre el nombre de usuario para ver los roles asignados al usuario. Para obtener más información sobre los usuarios basados en el rol, consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15. Haga clic para cerrar la sesión y, a continuación, inicie la sesión como un usuario diferente.
- J: actualmente, el archivo de ayuda contextual se muestra solo para la página en que se encuentra y no las páginas de inicio del portal. Haga clic para obtener instrucciones basadas en tareas para utilizar de forma eficaz vínculos, botones, cuadros de diálogo, asistentes y páginas en OpenManage Enterprise.
- K: haga clic en esta opción para ver la versión actual de OpenManage Enterprise instalada en el sistema. Haga clic en **Licencias** para leer el mensaje. Haga clic en los vínculos correspondientes para ver y descargar archivos de código abierto relacionados con OpenManage Enterprise u otras licencias de código abierto.
- L: haga clic en el símbolo para fijar o quitar los elementos de menú. Para fijar elementos de menú, expanda el menú **OpenManage Enterprise** y haga clic en el símbolo de alfiler.

Los datos sobre los elementos que se muestran en una tabla pueden verse en su totalidad, exportarse totalmente o basarse en los elementos seleccionados. Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50. Cuando se visualizan en texto azul, se puede ver y actualizar la información detallada sobre los elementos en una tabla, la que se abre en la misma ventana o en una página separada. Los datos tabulados se pueden filtrar mediante la característica **Filtros avanzados**. Los filtros varían según el contenido que sea vea. Ingrese o seleccione datos de los campos. Los números o el texto sin completar no mostrarán resultados esperados. Los datos que coinciden con los criterios de filtro aparecen en la lista. Para quitar los filtros, haga clic en **Borrar todos los filtros**.

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

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

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

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

Una vez conectado, todas las páginas se actualizan automáticamente. Si durante los inicios de sesión subsiguientes a la implementación del dispositivo se encuentra disponible una versión actualizada de OpenManage Enterprise, recibirá una alerta para actualizar la versión inmediatamente haciendo clic en **Actualizar**. Los usuarios con todos los privilegios de OpenManage Enterprise (administrador, administrador de dispositivos y observador) pueden ver el mensaje, pero solo un administrador puede actualizar la versión. Un administrador puede optar por obtener el recordatorio más tarde o descartar el mensaje. Para obtener más información acerca de la actualización de la versión de OpenManage Enterprise, consulte [Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles](#) en la página 150.

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](#) en la página 105.

Información relacionada

[Implementación y administración de OpenManage Enterprise](#) en la página 18

Portal de inicio de OpenManage Enterprise

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

- Vea el panel para obtener una instantánea en vivo sobre los estados de la condición de los dispositivos y, a continuación, lleve a cabo acciones, según sea necesario. Consulte [Panel](#).
- Vea las alertas de las categorías Crítico y Advertencia, y resuélvalas. Consulte [Administración de alertas de dispositivos](#).
- La sección de widgets indica los estados consolidados de la garantía, el cumplimiento del firmware o los controladores y el nivel de cumplimiento de la configuración de todos los dispositivos.

Para obtener más información sobre las características en Widgets, consulte [Supervisión de dispositivos mediante el tablero de OpenManage Enterprise](#) en la página 35. 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](#) en la página 93 y [Utilización de trabajos para el control de dispositivos](#) en la página 105.

- Si se encuentra disponible una versión actualizada de OpenManage Enterprise, se alerta inmediatamente cuando haya una actualización disponible. Para actualizar, haga clic en **Actualizar**. Para obtener más información acerca de la actualización de la versión de OpenManage Enterprise, consulte [Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles](#) en la página 150.
- 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](#) en la página 105.

Temas:

- [Supervisión de dispositivos mediante el tablero de OpenManage Enterprise](#)
- [Organizar los dispositivos en grupos](#)
- [Gráfico de anillo](#)
- [Estados de los dispositivos](#)

Supervisión de dispositivos mediante el tablero 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](#) en la página 15.

Además del primer inicio de sesión, el panel es la primera página que se ve después de cada inicio de sesión subsiguiente en OpenManage Enterprise. Para abrir la página Panel en cualquier página de OpenManage Enterprise, haga clic en el símbolo del panel ubicado en la esquina superior izquierda. De manera alternativa, haga clic en **Inicio**. Con el uso de los datos de supervisión en tiempo real, en el panel se muestra la condición del dispositivo, el cumplimiento del firmware o los controladores, la garantía, las alertas y otros aspectos de los dispositivos y grupos de dispositivos que se encuentran en el entorno del centro de datos. En el panel también se muestran las actualizaciones disponibles de la consola. Puede actualizar la versión de OpenManage Enterprise inmediatamente o configurar OpenManage Enterprise para que se lo recuerde posteriormente. De manera predeterminada, cuando se conecta a la aplicación por primera vez, aparece en blanco la página Panel. Agregue dispositivos a OpenManage Enterprise para que se puedan supervisar y mostrar en el panel. Para agregar dispositivos, consulte [Detección de dispositivos para la supervisión o administración](#) en la página 110 y [Organizar los dispositivos en grupos](#) en la página 36.

- [Administrar el firmware y los controladores del dispositivo](#) en la página 55
- [Administración de alertas de dispositivos](#)
- [Detección de dispositivos](#)
- [Creación de informes](#)
- [Administración de los ajustes del servidor OpenManage Enterprise](#) en la página 136

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](#) en la página 93. La cantidad total de alertas en el gráfico de anillo varía según la configuración de la vista de las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Consulte [Personalizar la visualización de alertas](#) en la página 149. 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](#) en la página 50. 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](#) en la página 50.

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

i **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](#) en la página 50.

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

- **Garantía:** muestra el número de dispositivos cuya garantía está por caducar. Esto se basa en la **Configuración de la garantía**. Si el usuario opta por la notificación de caducidad de la garantía, entonces se muestra la cantidad de dispositivos cuya garantía está vencida. De lo contrario, se muestra la cantidad que caduca pronto o el recuento de las garantías activas. Haga clic para ver más información en el cuadro de diálogo **Garantía**. Para obtener información sobre la administración de la garantía del dispositivo, consulte [Administración de la garantía del dispositivo](#) en la página 126. Detenga el puntero del mouse sobre la sección **Garantía** para leer las definiciones sobre los símbolos utilizados en la sección.
- **Firmware/Controladores:** muestra el estado de cumplimiento del firmware o los controladores de las bases de los dispositivos creadas en OpenManage Enterprise. Si están disponibles, en esta sección se muestran las bases de firmware y dispositivos marcadas como críticas y de advertencia.
 - Para obtener más información sobre el estado de resumen, consulte la documentación técnica *ADMINISTRACIÓN DEL ESTADO DE RESUMEN MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.
 - Haga clic para ver más información en la página **Cumplimiento del firmware/controlador**.
 - Para obtener información sobre la actualización de un firmware, la creación del catálogo de firmware, la creación de la línea base de firmware y la generación de un informe de cumplimiento de línea base, consulte [Administrar el firmware y los controladores del dispositivo](#) en la página 55.
- **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](#) en la página 87.

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](#) en la página 50.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos supervisados por OpenManage Enterprise. Haga clic en **OpenManage Enterprise > Supervisión > Informes > Informe de la descripción general de dispositivos**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

i **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](#) en la página 15.

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

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

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

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

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

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

- **Grupo de MCM:** indica el grupo de administración de varios chasis (MCM) que tiene más de un chasis identificado mediante la sintaxis siguiente: `Group_<MCM group name>_<Lead_Chassis_Svctag>` donde:
 - `<MCM group name>`: nombre del grupo de MCM
 - `<Lead_Chassis_Svctag>`: la etiqueta de servicio del chasis principal. El chasis, los sleds y los módulos de E/S de la red forman este grupo.
- **Grupo de chasis independiente:** se identifica usando la sintaxis `<Chassis_Svctag>`. El chasis, los sleds y los módulos de E/S de la red forman este grupo.
- **Dispositivos de red:** conmutadores del sistema de red Dell Force10 y los conmutadores del Fibre Channel
- **Servidores:** servidores Dell iDRAC, servidores Linux, servidores que no son Dell, servidores de OEM y servidores Windows
- **Dispositivos de almacenamiento:** arreglos de almacenamiento Dell Compellent, arreglos de almacenamiento PowerVault MD y arreglos de almacenamiento PowerVault ME
- **Grupos de detección:** grupos que se asignan al intervalo de una tarea de detección. No se puede editar ni eliminar porque el grupo está bajo el control del trabajo de detección donde se aplica la condición incluir/excluir. Consulte [Detección de dispositivos para la supervisión o administración](#) en la página 110.

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.
- Cuando se implementan cambios en un grupo estático (se agregan o eliminan dispositivos) o en un grupo de consulta (cuando se actualiza una consulta), el cumplimiento del firmware o los controladores de los dispositivos asociados con estos grupos no se actualiza automáticamente. Se recomienda que el usuario inicie un cumplimiento de firmware o controladores para los dispositivos agregados o eliminados recientemente en dichas instancias.

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

En la página **Todos los dispositivos**, en el panel izquierdo, puede crear grupos secundarios en el grupo principal estático y de consultas. Consulte [Crear o eliminar un grupo estático de dispositivos](#) en la página 42 y [Crear o editar un grupo de dispositivos de consulta](#) en la página 43.

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](#) en la página 15.

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](#) en la página 46

[Actualizar el inventario de dispositivos](#) en la página 48

[Actualizar el estado del dispositivo](#) en la página 48

Gráfico de anillo

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

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

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


- Estados de alerta de los dispositivos: indican el total de alertas generadas para los dispositivos que supervisa OpenManage Enterprise. Consulte [Supervisión de alertas de dispositivos](#) en la página 93.

NOTA: La cantidad total de alertas en el gráfico de anillo varía según la configuración de la vista de las alertas no confirmadas. De manera predeterminada, solo se muestran las alertas no confirmadas. Consulte [Personalizar la visualización de alertas](#) en la página 149.

- Para conocer el cumplimiento de la versión de firmware de un dispositivo en comparación con la versión del catálogo, consulte [Administrar el firmware y los controladores del dispositivo](#) en la página 55.
- Para conocer la línea base de cumplimiento de la configuración de los dispositivos y grupos de dispositivos, consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.

NOTA: El nivel de cumplimiento del dispositivo seleccionado se indica en un gráfico de anillo. Cuando más de un dispositivo está relacionado con una línea base, el estado de un dispositivo con el nivel de cumplimiento más bajo con respecto a la línea base se indica como el mismo nivel de cumplimiento de dicha línea base. Por ejemplo, si varios dispositivos están relacionados con una línea base de firmware y el nivel de cumplimiento de algunos dispositivos es





Correcto  o Cambiar a una versión anterior , pero si el cumplimiento de un dispositivo en el grupo es Actualizar


, el nivel de cumplimiento del firmware de base se indica como Actualizar. El estado de resumen es igual al estado del dispositivo que tiene alta gravedad. Para obtener más información sobre el estado de resumen, consulte la documentación técnica *ADMINISTRACIÓN DEL ESTADO DE RESUMEN MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.

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

Estados de los dispositivos

Tabla 12. Estados de los dispositivos en OpenManage Enterprise

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

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

Administración de dispositivos

Haga clic en **OpenManage Enterprise > Dispositivos** para 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:

- **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](#) en la página 15.**
- **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.**
- **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](#) en la página 50.**
- **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>.**

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](#) en la página 46.
- Excluir un dispositivo de la supervisión de OpenManage Enterprise. Consulte [Excluir dispositivos de OpenManage Enterprise](#) en la página 46.
- 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](#) en la página 50.
- 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](#) en la página 54.

Para las tareas relacionadas con grupos de dispositivos, consulte [Organizar los dispositivos en grupos](#) en la página 36.

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. En **Acciones rápidas**, se indican los

vínculos de administración que se relacionan con el dispositivo correspondiente. Para borrar las selecciones, haga clic en **Borrar selección**.

NOTA: 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](#)
- [Visualización y configuración de dispositivos](#)
- [Iniciar la aplicación de administración iDRAC de un dispositivo](#)
- [Iniciar la consola virtual](#)

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](#) en la página 50.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos supervisados por OpenManage Enterprise. Haga clic en **OpenManage Enterprise > Supervisión > Informes > Informe de la descripción general de dispositivos**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

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](#) en la página 15.

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

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

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

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

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

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

- **Grupo de MCM:** indica el grupo de administración de varios chasis (MCM) que tiene más de un chasis identificado mediante la sintaxis siguiente: `Group_<MCM group name>_<Lead_Chassis_Svctag>` donde:
 - `<MCM group name>`: nombre del grupo de MCM
 - `<Lead_Chassis_Svctag>`: la etiqueta de servicio del chasis principal. El chasis, los sleds y los módulos de E/S de la red forman este grupo.

- **Grupo de chasis independiente:** se identifica usando la sintaxis `<Chassis_Svctag>`. El chasis, los sleds y los módulos de E/S de la red forman este grupo.

- **Dispositivos de red:** conmutadores del sistema de red Dell Force10 y los conmutadores del Fibre Channel
- **Servidores:** servidores Dell iDRAC, servidores Linux, servidores que no son Dell, servidores de OEM y servidores Windows
- **Dispositivos de almacenamiento:** arreglos de almacenamiento Dell Compellent, arreglos de almacenamiento PowerVault MD y arreglos de almacenamiento PowerVault ME
- **Grupos de detección:** grupos que se asignan al intervalo de una tarea de detección. No se puede editar ni eliminar porque el grupo está bajo el control del trabajo de detección donde se aplica la condición incluir/excluir. Consulte [Detección de dispositivos para la supervisión o administración](#) en la página 110.

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.**
- **Cuando se implementan cambios en un grupo estático (se agregan o eliminan dispositivos) o en un grupo de consulta (cuando se actualiza una consulta), el cumplimiento del firmware o los controladores de los dispositivos asociados con estos grupos no se actualiza automáticamente. Se recomienda que el usuario inicie un cumplimiento de firmware o controladores para los dispositivos agregados o eliminados recientemente en dichas instancias.**

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

En la página **Todos los dispositivos**, en el panel izquierdo, puede crear grupos secundarios en el grupo principal estático y de consultas. Consulte [Crear o eliminar un grupo estático de dispositivos](#) en la página 42 y [Crear o editar un grupo de dispositivos de consulta](#) en la página 43.

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](#) en la página 15.

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](#) en la página 46

[Actualizar el inventario de dispositivos](#) en la página 48

[Actualizar el estado del dispositivo](#) en la página 48

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](#) en la página 15.

1. Haga clic con el botón derecho del ratón en **Grupos estáticos** y, a continuación, haga clic en **Crear nuevo grupo estático**. Por otra parte, haga clic en el ícono **+**, seleccione **Grupo estático** y haga clic en **Crear** en el cuadro de diálogo **Crear grupo personalizado**.
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 distinga 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](#) en la página 15.

1. Haga clic con el botón secundario en **Grupos de consulta** y, luego, haga clic en **Crear nuevo grupo de consulta**. Por otra parte, haga clic en el icono **+**, seleccione **Grupo de consulta** y haga clic en **Crear** en el cuadro de diálogo Crear grupo personalizado. Para conocer las definiciones de grupo estático o de consulta (dinámico), consulte [Organizar los dispositivos en grupos](#) en la página 36.
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](#) en la página 43.
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](#) en la página 130.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte [Crear o editar un grupo de dispositivos de consulta](#) en la página 43.

Defina los criterios de consulta mediante dos opciones:

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

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

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

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

1. En el cuadro de diálogo **Selección de criterios de consulta**, seleccione en el menú desplegable según si desea crear criterios de consulta para grupos de consulta o para generación de informes.
2. Agregue o quite un filtro haciendo clic en el símbolo más o en el símbolo de basurero, respectivamente.
3. Haga clic en **Finalizar**.
Se genera un criterio de consulta y se guarda en la lista de consultas existentes. Se realiza una entrada de registro de auditoría y aparece en la lista de los registros de auditoría. Consulte [Administrar registros de auditoría](#) en la página 103.

Información relacionada

[Administración del cumplimiento de la configuración del dispositivo](#) en la página 86

[Editar una línea base de cumplimiento de configuración](#) en la página 90

[Eliminar una línea base de cumplimiento de configuración](#) en la página 91

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](#) en la página 15.

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](#) en la página 36.
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](#) en la página 46 y [Dispositivos de exclusión global](#) en la página 117.

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](#) en la página 36.
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](#) en la página 15.

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](#) en la página 15.

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](#) en la página 50.
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

NOTA:

- Un dispositivo con un perfil asignado no se puede eliminar, a menos que se desasigne el perfil. Para obtener más información, consulte [Anular asignación de perfiles](#) en la página 83.
- Se puede eliminar un dispositivo incluso cuando se están ejecutando tareas en él. Las tareas que se inician en un dispositivo fallan si se elimina el dispositivo antes de su finalización.

Para eliminar los dispositivos descubiertos:

1. En el panel izquierdo, seleccione los dispositivos.
2. En la lista de dispositivos, seleccione la casilla de verificación correspondiente a los dispositivos y, luego, haga clic en **Eliminar**.
3. Cuando se le solicite indicar si los dispositivos se excluirán globalmente, haga clic en **Sí**. El dispositivo se elimina y OpenManage Enterprise deja de supervisarlos.

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.

Información relacionada

[Organizar los dispositivos en grupos](#) en la página 36

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](#) en la página 15.

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 el firmware y los controladores del dispositivo mediante las bases

Puede actualizar la versión del firmware o los controladores de los dispositivos en la página Todos los dispositivos o en la página Cumplimiento del firmware/controlador (consulte [Actualizar el firmware o los controladores con el informe de cumplimiento de la base](#) en la página 61). Se recomienda realizar la actualización mediante la página Todos los dispositivos cuando se actualiza el firmware y el controlador de un mismo dispositivo.

NOTA:

- Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15.

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

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

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

2. En el cuadro de diálogo **Actualizar dispositivo**:

a. En la sección **Seleccionar fuente de actualización**, seleccione una de las siguientes opciones:

- Seleccione la base en el menú desplegable **Base**. Aparecerá una lista de dispositivos relacionados con la base seleccionada. El nivel de cumplimiento de cada dispositivo se muestra en la columna “Cumplimiento”. Según el nivel de cumplimiento, puede actualizar la versión del controlador o el firmware. Para obtener más información sobre la descripción del campo en esta página, consulte [Visualización del informe de cumplimiento del firmware del dispositivo](#).
 - Seleccione las casillas de verificación correspondientes a los dispositivos que se deben actualizar.
 - Haga clic en **Siguiente**.
- También puede actualizar el firmware o los controladores mediante el paquete individual de actualización. Haga clic en **Paquete individual** y, a continuación, siga las instrucciones que aparecen en la pantalla. Haga clic en **Siguiente**.

b. En la sección **Programa**:

• En **Programar actualización**, haga clic en **Información adicional** para ver la información importante y seleccione una de las siguientes opciones:

- Actualizar ahora:** se aplican las actualizaciones del firmware o el controlador inmediatamente.
- Programar más tarde:** se utiliza para especificar una fecha y hora en que se deba actualizar la versión del firmware o el controlador. Este modo se recomienda si no desea alterar sus tareas actuales.

• En **Opciones del servidor**, seleccione una de las siguientes opciones de reinicio:

- Para reiniciar el servidor inmediatamente después de la actualización del firmware o controlador, seleccione **Reiniciar el servidor inmediatamente** y, en el menú desplegable, seleccione una de las siguientes opciones:
 - Reinicio ordenado sin apagado forzado**
 - Reinicio ordenado con apagado forzado**
 - Ciclo de encendido y apagado** para un restablecimiento forzado del dispositivo.
- Seleccione **Programar para el siguiente reinicio del servidor** a fin de activar la actualización del firmware o el controlador cuando se produzca el siguiente reinicio del servidor. Si se selecciona esta opción, se debe ejecutar manualmente la comprobación de la base y el inventario después de que el paquete esté instalado en el dispositivo remoto.

3. Haga clic en **Finalizar**.

Se crea un trabajo de actualización de firmware o controlador y aparece en la lista de trabajos. Consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105.



Reversar la versión del firmware de un dispositivo individual

Puede revertir la versión de firmware de un dispositivo que es posterior a la versión de firmware de la línea base a la que está asociado. Esta función solo está disponible cuando se ven y configuran las propiedades de un dispositivo individual. Consulte [Visualización y configuración de dispositivos](#) en la página 50. Puede actualizar o revertir la versión de firmware de un dispositivo individual. Puede revertir la versión de firmware de un solo dispositivo a la vez.

NOTA:

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

Cualquier firmware de dispositivo actualizado mediante el uso de la interfaz gráfica de usuario del iDRAC no aparece aquí en la lista y no se puede actualizar. Para obtener información acerca de la creación de la línea base, consulte [Crear una base](#) en la página 59.

1. En el panel izquierdo, seleccione el grupo y, a continuación, haga clic en el nombre del dispositivo en la lista.
 2. En la página **<nombre del dispositivo>**, haga clic en **Firmware/Controladores**.
 3. En el menú desplegable **Línea base**, seleccione la línea base a la que pertenece el dispositivo.
Se indican todos los dispositivos asociados con la línea base. Para obtener más información sobre la descripción de campo en la tabla, consulte [Ver el informe de cumplimiento de la base](#) en la página 60.
 4. Seleccione la casilla de verificación correspondiente al dispositivo cuya versión del firmware debe revertirse, el cual se identifica con  ..
 5. Haga clic en **Revertir firmware**.
 6. En el cuadro de diálogo **Revertir firmware**, se muestra la siguiente información:
 - **NOMBRE DEL COMPONENTE:** componente en el dispositivo cuya versión de firmware es posterior a la versión de línea base.
 - **VERSIÓN ACTUAL:** versión actual del componente.
 - **VERSIÓN DE LA REVERSIÓN:** versión de firmware sugerida a la que se puede degradar el componente.
 - **FUENTE DE REVERSIÓN:** haga clic en **Examinar** para seleccionar la fuente desde donde se puede descargar la versión de firmware.
 7. Haga clic en **Finalizar**. La versión del firmware se revierte.
-  **NOTA:** Actualmente, la función de reversión realiza un seguimiento solo del número de versión desde la que se revirtió el firmware. La reversión no considera la versión del firmware que esté instalada usando la función de reversión (revirtiendo la versión).

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](#) en la página 50. Para descargar un inventario del dispositivo, consulte [Exportar el inventario de un solo dispositivo](#) en la página 49.

Información relacionada

[Organizar los dispositivos en grupos](#) en la página 36

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](#) en la página 49.

Información relacionada

Organizar los dispositivos en grupos en la página 36

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](#) en la página 40.

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](#) en la página 39.
- **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](#) en la página 114.

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](#) en la página 50.

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](#) en la página 108.
- **CLI de RACADM:** haga clic en esta opción para ejecutar un comando de RACADM. Consulte [Crear un trabajo de comando remoto para la administración de dispositivos](#) en la página 108.
- **Actualizar firmware:** consulte [Actualizar el firmware y los controladores del dispositivo mediante las bases](#) en la página 46.
- **Incorporación:** consulte [Incorporación de dispositivos](#) en la página 114.
- **Exportar todo y seleccionados exportados:** Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50.

Información de hardware que se muestra para el chasis MX7000

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

Exportar todos los datos o aquellos seleccionados

Puede exportar datos:

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

NOTA: No obstante, un inventario de dispositivo único solo se puede exportar a un formato .csv. Consulte [Exportar el inventario de un solo dispositivo](#) en la página 49.

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](#) en la página 132.

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.

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

- Ver la información sobre el estado y el nivel de alimentación, la IP del dispositivo y la etiqueta de servicio.
- Ver información general sobre el dispositivo y realizar tareas de solución de problemas y de control del dispositivo.

- Ver la información de dispositivos, como RAID, PSU, OS, NIC, memoria, procesador y gabinete de almacenamiento. OpenManage Enterprise ofrece un informe integrado para obtener una descripción general acerca de la NIC, el BIOS, el disco físico y el disco virtual que se utilizan en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise > Monitorear > Informes**.
 - Actualizar o revertir las versiones de firmware de los componentes en un dispositivo que están relacionadas con una línea base de firmware. Consulte [Administrar el firmware y los controladores del dispositivo](#) en la página 55.
- NOTA:** La actualización de un dispositivo mediante el flujo de trabajo de paquete individual solo es compatible con los Dell Update Packages basados en archivos ejecutables (EXE). Cuando se actualiza un CMC de FX2, el DUP ejecutable se debe instalar a través de uno de los sled en el chasis.
- Confirmar, exportar, eliminar u omitir las alertas relacionadas con un dispositivo. Consulte [Administración de alertas de dispositivos](#).
 - Ver y exportar datos de registro del hardware de un dispositivo. Consulte [Administración de los registros de hardware de dispositivos individuales](#) en la página 53.
 - Ver y administrar el inventario de configuración del dispositivo para los fines de cumplimiento de la configuración. Se inicia una comparación de cumplimiento cuando el inventario de configuración se ejecuta respecto a los dispositivos.
 - Ver el nivel de cumplimiento de un dispositivo comparado con la línea base de cumplimiento de la configuración con la que se encuentra asociado. Consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.

Descripción general del dispositivo

- En la página **<device name>**, en **Descripción general**, se muestran el estado, el nivel de alimentación y la etiqueta de servicio del dispositivo. Haga clic en la dirección IP para abrir la página de inicio de sesión de iDRAC. Consulte la *Guía del usuario de iDRAC* disponible en el sitio de soporte de Dell.
 - **Información:** información del dispositivo, como la etiqueta de servicio, las ranuras DIMM, el nombre de DNS de iDRAC, los procesadores, el chasis, el sistema operativo y el nombre del centro de datos. Se indican varias direcciones IP de administración relacionadas con el dispositivo y se puede hacer clic en ellas para activar las interfaces correspondientes.
 - **Alertas recientes:** las últimas alertas que se generaron para el dispositivo.
 - **Actividad reciente:** una lista de los trabajos recientes ejecutados en el dispositivo. Haga clic en **Ver todos** para ver todos los trabajos. Consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105.
 - **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](#) en la página 52.
 - Restablezca el iDRAC.
 - Extraiga y descargue el informe de SupportAssist. Consulte [Extraer y descargar informes de SupportAssist](#) en la página 53.
 - Actualice el estado del dispositivo.
 - Actualice el inventario de dispositivos.
 - Exporte el inventario del dispositivo que se recopila. Para ello, haga clic en **Actualizar inventario**. Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50.
 - Ejecute un comando remoto de RACADM e IPMI en el dispositivo. Consulte [Ejecutar de forma remota de RACADM e IPMI de comandos en dispositivos individuales](#) en la página 53.

OpenManage Enterprise ofrece un informe incorporado para obtener una descripción general de los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise > Monitorear > Informes > Informe de la visión general de dispositivos**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

Información del hardware del dispositivo

OpenManage Enterprise ofrece un informe incorporado sobre los componentes y su cumplimiento con la línea base de cumplimiento del firmware. Haga clic en **OpenManage Enterprise > Monitorear > Informes > Cumplimiento de firmware por informe de componentes**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

- **Información de la tarjeta del dispositivo:** información sobre las tarjetas que se utilizan en el dispositivo.
- **Software instalado:** lista del firmware y el software instalados en los distintos componentes del dispositivo.

- **Procesador:** información del procesador, como zócalos, familia, velocidad, núcleos y modelo.
- **Información de la controladora RAID:** el controlador PERC y RAID que se utiliza en los dispositivos de almacenamiento. El resumen del estado es igual al estado de la RAID que tiene alta gravedad. Para obtener más información sobre el estado de Resumen de condición, consulte las notas técnicas *ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.ª GENERACIÓN Y POSTERIORES* en Dell TechCenter.
- **Información de NIC:** información sobre las NIC que se utilizan en el dispositivo.
- **Información de la memoria:** los datos sobre las DIMM que se utilizan en el dispositivo.
- **Disco de matriz:** información sobre las unidades instaladas en el dispositivo. OpenManage Enterprise ofrece un informe integrado sobre los discos duros o las unidades virtuales disponibles en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise > Monitorear > Informes > Informe del disco físico**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.
- **Controladora de almacenamiento:** la controladora de almacenamiento instalada en el dispositivo. Haga clic en el símbolo más para ver los datos individuales de la controladora.
- **Información de suministro de energía:** información sobre los suministros de energía instaladas en el dispositivo.
- **Sistema operativo:** OS instalado en el dispositivo.
- **Licencias:** estado de las distintas licencias instaladas en el dispositivo.
- **Gabinete de almacenamiento:** estado del gabinete de almacenamiento y de la versión de EMM.
- **Memoria flash virtual:** lista de unidades flash virtual y sus especificaciones técnicas.
- **FRU:** lista de las Unidades reemplazables de campo (FRU, por sus siglas en inglés) que pueden gestionar y reparar únicamente los técnicos de campo. OpenManage Enterprise ofrece un informe integrado sobre las unidades reemplazables en el campo (FRU) instaladas en los dispositivos que OpenManage Enterprise supervisa. Haga clic en **OpenManage Enterprise > Monitorear > Informes > Informe de FRU**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.
- **Información de administración de dispositivos:** información de la dirección IP de la iDRAC instalada solamente en el caso de un dispositivo de servidor.
- **Datos del huésped:** muestra los dispositivos huéspedes que OpenManage Enterprise supervisa. UUID es el identificador único universal del dispositivo. La columna **ESTADO DE LOS HUÉSPEDES** indica el estado de funcionamiento del dispositivo huésped.

Ejecutar y descargar informes de diagnóstico

- **NOTA:** Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
- **NOTA:** Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.

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

NOTA: Consulte el documento técnico *Diagnóstico automatizado en ejecución remota por medio de los comandos WS-Man y RACADM* en https://en.community.dell.com/techcenter/extras/m/white_papers/20438187.

3. Para generar el informe de diagnóstico en el momento, seleccione **Ejecutar ahora**.
4. Haga clic en **Aceptar**. Cuando se le solicite, haga clic en **Sí**.

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

Se crea un trabajo que se muestra en la página **Trabajos**. Para ver más información sobre un trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte [Ver la lista de trabajos](#) en la página 105. El estado del trabajo también se muestra en la sección **Actividad reciente**. Cuando se haya ejecutado correctamente el trabajo, el estado del trabajo se indica como **Diagnóstico terminado** y el vínculo **Descargar** se muestra en la sección **Actividad reciente**.

5. Para descargar el informe, haga clic en el vínculo **Descargar** y, a continuación, descargue el archivo del informe de diagnósticos **<Servicetag-jobid>.TXT**.
 - De lo contrario, haga clic en **Solucionar problemas > Descargar informe de diagnóstico** y, a continuación, descargue el archivo.

6. En el cuadro de diálogo **Descargar archivos RemoteDiagnostics**, haga clic en el enlace de archivos .TXT y, a continuación, descargue el informe.
7. Haga clic en **Aceptar**.

Extraer y descargar informes de SupportAssist

- NOTA:** Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15
 - NOTA:** Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.
1. En la página **<Nombre del dispositivo>**, en el menú desplegable **Solucionar problemas**, seleccione **Extraer informe de SupportAssist**.
 2. En el cuadro de diálogo **Extraer informe de SupportAssist**:
 - a. Ingrese el nombre del archivo donde se debe guardar el informe de SupportAssist.
 - b. Seleccione las casillas de verificación correspondientes a los tipos de registro de los cuales se debe extraer un informe de SupportAssist.
 3. Haga clic en **Aceptar**.
Se crea un trabajo que se muestra en la página **Trabajos**. Para ver más información sobre un trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte [Ver la lista de trabajos](#) en la página 105. El estado del trabajo también se muestra en la sección **Actividad reciente**. Cuando se haya ejecutado correctamente el trabajo, el estado del trabajo se indica como **Diagnóstico terminado** y el vínculo **Descargar** se muestra en la sección **Actividad reciente**.
 4. Para descargar el informe, haga clic en el vínculo **Descargar** y, a continuación, descargue el archivo del informe de SupportAssist **<Service Tag>.<Time>.TXT**.
 - De lo contrario, haga clic en **Solucionar problemas > Descargar informe de SupportAssist**.
 5. En el cuadro de diálogo **Descargar archivos SupportAssist**, haga clic en el enlace de archivos .TXT y, a continuación, descargue el informe. Cada vínculo representa el tipo de registro que seleccionó.
 6. Haga clic en **Aceptar**.

Administración de los registros de hardware de dispositivos individuales

- NOTA:** Los registros de hardware están disponibles para los servidores YX4X, chasis MX7000 y sleds. Consulte [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.
- En la página **<nombre del dispositivo>**, haga clic en **Registros de hardware**. Se indican todos los sucesos y los mensajes de error generados para el dispositivo. Para obtener descripciones sobre campos, consulte [Administrar registros de auditoría](#) en la página 103.
 - Para un chasis, los datos en tiempo real sobre los registros de hardware se recuperan del chasis.
 - Para agregar un comentario, haga clic en **Agregar comentario**.
 - En el cuadro de diálogo, escriba el comentario y, a continuación, haga clic en **Guardar**. El comentario se guarda y se identifica por un símbolo en la columna **COMENTARIO**.
 - Para exportar los datos de registro seleccionados a un archivo .CSV, seleccione las casillas de verificación que correspondan y, a continuación, haga clic en **Exportar > Exportar seleccionado**.
 - Para exportar todos los registros en una página, haga clic en **Exportar > Exportar Página actual**.

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

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

- NOTA:** El uso de la CLI de RACADM solo permite un comando a la vez.

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

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

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

NOTA: Ingrese un comando de IPMI con la siguiente sintaxis: `-I lanplus <command>`

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](#) en la página 105.
5. Haga clic en **Finalizar**.
La sección **Alertas recientes** muestra el estado de finalización del trabajo.

Iniciar la aplicación de administración iDRAC de un dispositivo

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

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

NOTA: También puede iniciar la aplicación de administración haciendo clic en la dirección IP en la lista de dispositivos. Consulte [Lista de dispositivos](#) en la página 49.

Iniciar la consola virtual

El vínculo **Consola virtual** funciona con la licencia de iDRAC Enterprise de los servidores YX4X. En los servidores YX2X y YX3X, el vínculo funciona con las versiones 2.52.52.52 y posteriores de la licencia de iDRAC Enterprise. Haga clic en el vínculo cuando el tipo actual del complemento de la consola virtual es Active X para ver un mensaje de petición, que indica que actualice la consola para HTML 5 para mejorar la experiencia del usuario. Consulte [Crear un trabajo para cambiar el tipo de complemento de la consola virtual](#) en la página 108 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener información.

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





Administrar el firmware y los controladores del dispositivo

En la página **OpenManage Enterprise > Configuración > Cumplimiento del firmware/controlador**, puede administrar el firmware de todos los dispositivos “administrados”. Con la versión 3.4 de OpenManage Enterprise, también puede actualizar los controladores de los dispositivos basados en Windows.

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](#) en la página 15. Para administrar estas configuraciones, debe contar con credenciales de nivel de administrador de OpenManage Enterprise.**
- **Si la versión del firmware o el controlador del dispositivo es anterior a la versión de la base, no se actualiza automáticamente y el usuario debe iniciar la actualización.**
- **Se recomienda actualizar el firmware y los controladores durante los períodos de mantenimiento para evitar que los dispositivos o el entorno se queden offline durante el horario comercial.**
- **Para administrar el firmware o los controladores de un dispositivo, el estado de incorporación del sistema debe ser “Administrado” o “Administrado con alertas”. Consulte [Incorporación de dispositivos](#) en la página 114**
- **Actualmente, el catálogo contiene controladores únicamente para los dispositivos basados en Windows de 64 bits.**

Con la función Firmware/controlador, puede:

- Utilizar un catálogo de firmware y controladores de Dell.com, ya sea de forma directa o después de guardarlo en una ruta de red. Consulte [Agregar un catálogo con Dell.com](#) en la página 56 o [Creación de un catálogo de firmware mediante una red local](#).
- Crear una base de firmware y controladores mediante los catálogos disponibles. Estas bases sirven como referencias para comparar la versión del firmware y el controlador de los dispositivos con la versión que se encuentra en el catálogo. Consulte [Creación de la línea base de firmware](#).
- Ejecutar un informe de cumplimiento para comprobar si los dispositivos relacionados con la base cumplen con las versiones del controlador y el firmware de la base. Consulte [Comprobación de cumplimiento del firmware](#). La columna **CUMPLIMIENTO** muestra:
 - **Correcto**  si la versión del firmware o los controladores del dispositivo objetivo es la misma que la de la base.
 - **Actualización:** si el dispositivo objetivo tiene una o varias versiones anteriores a la versión del controlador o el firmware de la línea de base. Consulte [Actualización de la versión de firmware del dispositivo](#)
 - **Crítico**  Si el dispositivo no cumple con la base e indica que es una actualización crítica, y el firmware y los controladores del dispositivo deben actualizarse para garantizar un correcto funcionamiento.
 - **Advertencia**  Si el firmware o los controladores del dispositivo no cumplen con la base y el firmware puede actualizarse para mejorar su funcionamiento.
 - **Cambio a una versión anterior**  Si el firmware o los controladores del dispositivo son posteriores a la versión de la base.
 - Exportar el informe de cumplimiento para fines estadísticos y de análisis.
 - Actualizar la versión del firmware o los controladores del dispositivo mediante la base. Consulte [Actualizar el firmware y los controladores del dispositivo mediante las bases](#) en la página 46

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](#) en la página 50.

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

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

Temas:

- [Administrar catálogos de firmware y controladores](#)
- [Crear una base](#)
- [Eliminar bases](#)
- [Editar una base](#)
- [Comprobar el cumplimiento del firmware y los controladores de un dispositivo](#)

Administrar catálogos de firmware y controladores

Los catálogos son paquetes de firmware y controladores basados en los tipos de dispositivos. En Dell.com se encuentran validados y publicados todos los catálogos disponibles (paquetes actualizados). Puede utilizar el catálogo directamente desde el repositorio en línea o puede descargarlo a un recurso compartido de red. Con estos catálogos, puede crear bases de firmware o controladores para los dispositivos detectados y comprobar su nivel de cumplimiento. Esta práctica reduce el esfuerzo adicional de los administradores y los administradores de dispositivos y también reduce el tiempo general que demoran las actualizaciones y el mantenimiento. Para obtener información sobre definiciones de campos en la página Catálogo de administración, consulte [Definiciones de campos de administración de catálogos](#) en la página 165. Los orígenes de catálogo a los que puede acceder en la actualidad son los siguientes:

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

NOTA: La administración de catálogos de firmware mediante Dell.com o una ruta de red local se limita solo al catálogo de Enterprise Server.

Agregar un catálogo 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](#) en la página 15.

NOTA: Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.

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

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

Se crea un nuevo catálogo de firmware y se agrega en la tabla Catálogo de la página **Administración de catálogos**.

3. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

Agregar un catálogo a la red local

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

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

i **NOTA: Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea de firmware que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.**

· NFS

- i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
- ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *nfsshare\catalog.xml*

· CIFS

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

· HTTP

- i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
- ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *compute/catalog.xml*.

· HTTPS

- i. En la casilla **Dirección de recurso compartido**, ingrese la dirección IP del sistema en el que se almacena el catálogo de firmware en la red.
- ii. En la casilla **Ruta del archivo de catálogo**, ingrese la ruta completa de la ubicación del archivo de catálogo. Ruta de ejemplo: *compute/catalog.xml*.
- iii. En la casilla **Nombre de usuario**, ingrese el nombre de usuario del dispositivo en el que se almacena el catálogo.
- iv. En la casilla **Contraseña**, ingrese la contraseña del dispositivo en el que se almacena el catálogo.
- v. Seleccione la casilla de verificación **Comprobación de certificado**.

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

- d. Después de introducir la **Dirección del recurso compartido** y la **Ruta del archivo del catálogo**, aparece el vínculo **Probar ahora**. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se establece la conexión con el catálogo, aparecerá el mensaje *Conexión correcta*. Si no se establece la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparecerá el mensaje *Error de conexión a la ruta*. Este paso es opcional.
 - e. En la casilla **Actualizar catálogo**, seleccione **Manual** o **Automático**.
Si el **Catálogo de actualizaciones** se selecciona como **Automáticamente**, seleccione **Diariamente** o **Semanalmente** como la frecuencia de actualización e ingrese la hora en formato de 12 horas.
3. Haga clic en **Finalizar**. El botón **Finalizar** aparece solo después de que ha completado todos los campos en el cuadro de diálogo. Se crea un nuevo catálogo de firmware y se agrega en la tabla Catálogo de la página **Administración de catálogos**.
 4. Para volver a la página **Cumplimiento del firmware/controlador**, haga clic en **Volver al cumplimiento del firmware/controlador**.

Tareas relacionadas

[Eliminar un catálogo](#) en la página 58

Información del certificado SSL

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

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

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

Acciones

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

Actualizar un catálogo

Los catálogos de firmware y controladores existentes se pueden actualizar desde el sitio Dell.com o los Dell Update Package (DUP), ubicados en el recurso compartido de red.

Para actualizar un catálogo, siga estos pasos:

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

Editar un catálogo

1. En la página **Administración de catálogos**, seleccione un catálogo.
Los detalles del catálogo se muestran en el panel derecho **<nombre del catálogo>**.
2. Haga clic en **Editar** en el panel derecho.
3. En el asistente **Editar catálogo de actualización**, edite las propiedades.
Las propiedades que no puede editar aparecen atenuadas. Para obtener información sobre definiciones de campos, consulte [Agregar un catálogo con Dell.com](#) en la página 56 y [Agregar un catálogo a la red local](#) en la página 56.
4. Ingrese la **Dirección del recurso compartido** y la **Ruta del archivo del catálogo**, aparece el vínculo **Probar ahora**. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se estableció la conexión con el catálogo, aparece un mensaje que indica `Connection Successful`. Si no se ha establecido la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparece el mensaje de error `Connection to path failed`. Este paso es opcional.
5. En la casilla **Actualizar catálogo**, seleccione **Manual** o **Automático**.
Si el **Catálogo de actualizaciones** se selecciona como **Automáticamente**, seleccione **Diariamente** o **Semanalmente** como la frecuencia de actualización e ingrese la hora en formato de 12 horas.
6. Haga clic en **Finalizar**.
Se crea y ejecuta inmediatamente un trabajo de detección. El estado del trabajo se indica en la columna **UBICACIÓN DEL REPOSITORIO** de la página **Administración de catálogos**.

Eliminar un catálogo

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

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

Información relacionada

[Agregar un catálogo a la red local](#) en la página 56

Crear una base

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

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15.

NOTA: No se actualizarán automáticamente los dispositivos que no cumplan con una versión del firmware o los controladores que sea anterior a la versión del catálogo. Debe actualizar la versión del firmware. Se recomienda actualizar el firmware de un dispositivo durante las ventanas de mantenimiento para evitar que los dispositivos o el entorno queden sin conexión durante el horario comercial.

1. En **Firmware**, haga clic en **Crear línea base**.
2. En el cuadro de diálogo **Crear base de actualización**:
 - a. En la sección **Información de línea base**:
 - i. En el menú desplegable **Catálogo**, seleccione un catálogo.
 - ii. Para agregar un catálogo a esta lista, haga clic en **Agregar**. Consulte [Administración de los catálogos de firmware](#).
 - iii. En la casilla **Nombre de línea base**, ingrese un nombre para la línea base y, a continuación, ingrese una descripción de la línea base.
 - iv. Haga clic en **Siguiente**.
 - b. En la sección **Destino**:
 - Para seleccionar uno o más dispositivos de destino:
 - i. Seleccione **Seleccionar dispositivos**, y, a continuación, haga clic en el botón **Seleccionar dispositivos**.
 - ii. En el cuadro de diálogo **Seleccionar dispositivos**, todos los dispositivos supervisados por OpenManage Enterprise, los módulos de E/S y los dispositivos en grupos estáticos o de consulta se muestran en los grupos correspondientes.
 - iii. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
 - iv. Seleccione la casilla de verificación correspondiente a los dispositivos. Los dispositivos seleccionados se indican bajo la pestaña **Dispositivos seleccionados**.
 - Para seleccionar uno o más grupos de dispositivos de destino:
 - i. Seleccione **Seleccionar grupos**, y, a continuación, haga clic en el botón **Seleccionar grupos**.
 - ii. En el cuadro de diálogo **Seleccionar grupos**, todos los dispositivos supervisados por OpenManage Enterprise, los módulos de E/S y los dispositivos en grupos estáticos o de consulta se muestran en las categorías correspondientes.
 - iii. En el panel izquierdo, haga clic en el nombre de la categoría. Los dispositivos de esa categoría se muestran en el panel de trabajo.
 - iv. Seleccione la casilla de verificación correspondiente a los grupos. Los grupos seleccionados se indican bajo la pestaña **Grupos seleccionados**.
3. Haga clic en **Finalizar**.

De este modo, se muestra un mensaje en que se indica que se creó un trabajo para crear la línea base.

En la tabla Línea base, aparecen los datos sobre el dispositivo y el trabajo de línea base. Para obtener información sobre definiciones de campos, consulte [Definiciones de los campos de la línea base de firmware](#) en la página 161.

Eliminar bases

Puede eliminar las bases de los dispositivos en la página **Configuración > Cumplimiento del firmware/controlador** y desvincular los dispositivos de los catálogos asociados.

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](#) en la página 15

Para eliminar las bases, siga estos pasos:

1. Seleccione las bases entre las que se enumeran en la página Cumplimiento del firmware/controlador.

2. Haga clic en **Eliminar** y, a continuación, en **Sí** en el mensaje de confirmación.

Las bases eliminadas se eliminan de la página Cumplimiento del firmware/controlador.

Editar una base

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

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


Comprobar el cumplimiento del firmware y los controladores de un dispositivo

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

NOTA:

- **Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15.**
- **El firmware y los controladores (Windows de 64 bits) para los dispositivos de la base que no cumplen con los requisitos no se actualizan automáticamente, por lo que el usuario debe actualizarlos. Se recomienda actualizar el firmware y los controladores de un dispositivo durante los períodos de mantenimiento para evitar que los dispositivos o el entorno se queden offline durante el horario comercial.**
- **Para recolectar la información del inventario, el Recolector de inventario y la Actualización del sistema Dell deben estar disponibles en el servidor de Windows. Si estos componentes no están disponibles en el servidor, inicie un trabajo de inventario y seleccione Recolectar inventario de los controladores. El trabajo de detección también recolecta información de inventario de los controladores, pero solo el trabajo de inventario instala los componentes necesarios en el servidor. Para recolectar la información del inventario del controlador, cree o edite un trabajo de inventario y seleccione la casilla de verificación Recolectar inventario de los controladores. Para obtener más información, consulte [Creación de un trabajo de inventario](#) en la página 123 y [Edición de un trabajo de programa de inventario](#) en la página 125.**

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

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

En la tabla Línea base, aparecen los datos sobre el dispositivo y el trabajo de línea base. Para obtener información sobre definiciones de campos, consulte [Definiciones de los campos de la línea base de firmware](#) en la página 161.


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

Consulte [Visualización del informe de cumplimiento del firmware del dispositivo](#).

 **NOTA:** La reversión no es compatible con los controladores.

Ver el informe de cumplimiento de la base

En la página **Configuración > Cumplimiento del firmware/controlador**, se indica el estado de cumplimiento de las bases. El gráfico de anillo proporciona un resumen del cumplimiento de las bases para sus respectivos catálogos. Cuando más de un dispositivo está relacionado con una base, el estado del dispositivo con el nivel de cumplimiento más bajo con respecto a la base se indica como el nivel de

cumplimiento de esa base. Por ejemplo, el nivel de cumplimiento de una base aparece como “Crítico” si esta tiene un solo dispositivo cuyo cumplimiento está marcado como “Crítico”,  incluso si la mayoría de los dispositivos está en cumplimiento.

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

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


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

NOTA: Si cada dispositivo tiene su propio estado, el estado de máxima gravedad se considera como el estado del grupo. Para obtener más información sobre el estado de Resumen de condición, consulte las notas técnicas **ADMINISTRACIÓN DEL RESUMEN DE CONDICIÓN ESTADO MEDIANTE EL USO DE IDRAC EN LOS SERVIDORES POWEREDGE DE DELL EMC DE 14.a GENERACIÓN Y POSTERIORES** en Dell TechCenter.

- **CUMPLIMIENTO:** indica el nivel de cumplimiento de un dispositivo con respecto a la línea base. Para obtener más información sobre los símbolos que se utilizan para analizar los niveles de cumplimiento del firmware o los controladores del dispositivo, consulte [Administrar el firmware y los controladores del dispositivo](#) en la página 55.
- **TIPO:** tipo de dispositivo en que se genera el informe de cumplimiento.
- **COMPONENTES Y NOMBRE DEL DISPOSITIVO:** de manera predeterminada, se aparece la etiqueta de servicio del dispositivo.
 1. Para ver información acerca de los componentes del dispositivo, haga clic en el símbolo **>**.

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

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

2. Seleccione una o varias casillas de verificación correspondientes a los dispositivos cuyo estado de cumplimiento del firmware sea “Crítico” y requieran una actualización.
 3. Haga clic en **Hacer compatible**. Consulte [Actualizar la versión de firmware del dispositivo usando el informe de cumplimiento de la base](#).
- **Etiqueta de Servicio:** haga clic en esta opción para ver información detallada sobre el dispositivo en la página **<nombre del dispositivo>**. Para obtener más información sobre las tareas que puede completar en esta página, consulte [Visualización y configuración de dispositivos](#) en la página 50.
 - **SOLICITUD DE REINICIO:** indica si el dispositivo se debe reiniciar después de actualizar el firmware.
 - **Información** : símbolo correspondiente a cada componente del dispositivo que esté vinculado a la página del sitio de soporte desde la que se puede actualizar el firmware o los controladores. Haga clic en este botón para abrir la página Detalles del controlador correspondiente en el sitio de soporte técnico.
 - **VERSIÓN ACTUAL:** indica la versión actual del firmware del dispositivo.
 - **VERSIÓN DE BASE:** indica la versión correspondiente del firmware y los controladores del dispositivo disponible en el catálogo asociado.
 - Para exportar el informe de cumplimiento a un archivo de Excel, seleccione las casillas de verificación correspondientes con el dispositivo y, a continuación, seleccione **Exportación**.
 - Para volver a la página **Firmware**, haga clic en **Volver a firmware**.
 - Para ordenar los datos en función de una columna, haga clic en el título de la columna.
 - Para buscar un dispositivo en la tabla, haga clic en **Filtros avanzados** y seleccione o ingrese datos en las casillas de filtrado. Consulte la opción Filtros avanzados en [Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise](#) en la página 33.

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

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

Actualizar ( o .

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

Al actualizar el chasis y sled MX7000 que pertenecen al grupo de administración de varios chasis (MCM), debe tener en cuenta lo siguiente:

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

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

- Tenga en cuenta que no se admite la reversión de las actualizaciones del controlador.
- Las actualizaciones de los controladores dentro de banda solo se admiten en Windows con OpenSSH. No se admiten actualizaciones de controladores en SSH alojados en Windows de otros fabricantes, como el CygwinSSH.
- Para recolectar la información del inventario, el Recolector de inventario y la Actualización del sistema Dell deben estar disponibles en el servidor de Windows. Si estos componentes no están disponibles en el servidor, inicie un trabajo de inventario y seleccione **Recolectar inventario de los controladores**. El trabajo de detección también recolecta información de inventario de los controladores, pero solo el trabajo de inventario instala los componentes necesarios en el servidor. Para recolectar la información del inventario del controlador, cree o edite un trabajo de inventario y seleccione la casilla de verificación **Recolectar inventario de los controladores**. Para obtener más información, consulte [Creación de un trabajo de inventario](#) en la página 123 y [Edición de un trabajo de programa de inventario](#) en la página 125.

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](#) en la página 15.**
- **Cree una regla de firewall entrante para habilitar la comunicación con el puerto 22.**
- **Si los recursos compartidos HTTP y HTTPS se ajustaron mediante la configuración de proxy, asegúrese de que estas direcciones URL locales se incluyan en la lista de excepciones del proxy antes de iniciar cualquier tarea de actualización.**
- **Solo se puede iniciar una tarea de actualización en la máquina objetivo en un momento determinado.**
- **Si se crean los trabajos de actualización de firmware o controlador con la opción “Programar para el siguiente reinicio del servidor”, se debe ejecutar manualmente la comprobación de la base y el inventario después de instalar el paquete en el dispositivo remoto.**
- **La función Restablecer iDRAC no es compatible con los dispositivos en un chasis MCM que se encuentran en estado de incorporación “Por proxy” y que solo se utilizan para actualizar los controladores de los dispositivos. Para obtener más información sobre los estados de incorporación, consulte [Incorporación de dispositivos](#) en la página 114.**


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

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

En la página **Informe de cumplimiento** aparece la lista de dispositivos relacionados con la base y su nivel de cumplimiento. Para obtener descripciones sobre campos, consulte [Ver el informe de cumplimiento de la base](#) en la página 60.

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

- **Borrar cola de trabajos:** seleccione esta opción para borrar todos los trabajos (programados, completados y fallidos) antes de que se inicie el trabajo de actualización en el dispositivo objetivo.

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

- **Restablecer la iDRAC:** seleccione esta opción para comenzar un reinicio de la iDRAC antes de que se inicie el trabajo de actualización.

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

5. Haga clic en **Actualizar**.

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

Administrar las plantillas de configuración de dispositivos

En la página **Plantillas de > configuración**, puede configurar los servidores y el chasis mediante las plantillas de configuración de dispositivos (predefinidas o personalizadas). Las plantillas le permiten optimizar los recursos de centro de datos y reducir el tiempo de ciclo en la creación de clones e implementaciones. Las plantillas mejoran sus operaciones de negocios críticas en infraestructura convergente que utilizan infraestructuras definidas por software.

Temas:

- [Crear una plantilla desde un dispositivo de referencia](#)
- [Crear una plantilla importando un archivo de plantilla](#)
- [Ver la información de una plantilla](#)
- [Editar una plantilla de servidor](#)
- [Editar una plantilla de chasis](#)
- [Editar plantilla de IOA](#)
- [Editar las propiedades de red](#)
- [Implementar las plantillas de dispositivos](#)
- [Implementar las plantillas de IOA](#)
- [Clonar plantillas](#)
- [Implementación automática de la configuración en servidores o chasis que aún no se han descubierto](#)
- [Crear destinos de implementación automática](#)
- [Eliminar destinos de implementación automática](#)
- [Exportar detalles del destino de implementación automática a diferentes formatos](#)
- [Descripción general de la implementación sin estado](#)
- [Definir redes](#)
- [Editar o eliminar una red configurada](#)
- [Exportar definiciones de VLAN](#)
- [Importar definiciones de red](#)

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](#) en la página 15.

NOTA: Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165.

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 > Plantillas > Crear plantilla** y, luego, seleccione **Desde dispositivo de referencia**.
2. En el cuadro de diálogo **Crear plantilla**:
 - a. En la sección **Información de la plantilla**, ingrese un nombre y una descripción para la plantilla de 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.

- **Clonar IOA de referencia:** le permite clonar la configuración de un agregador M de I/O existente.

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

- Haga clic en **Siguiente**.
- 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.

NOTA: Solo las plantillas de IOA que se extrajeron en el momento de la detección del chasis están disponibles para la clonación. Consulte [Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección](#) en la página 118

- 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. De forma predeterminada, se seleccionan todos los elementos.
- 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 **Monitorear > Trabajos** Para ver información adicional sobre el trabajo, selecciónelo y luego haga clic en **Ver detalles** en el panel de trabajo. En la página **Detalles del trabajo**, aparecen los detalles de ejecución del trabajo. En el panel **Resultados**, haga clic en **Ver detalles** para ver información detallada de la ejecución del trabajo.

Crear una plantilla importando un archivo de plantilla

NOTA: Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.

- En el menú **OpenManage Enterprise**, haga clic en **Configuración > Plantillas > Crear plantilla** y, luego, seleccione **Importar desde archivo**.
- En el cuadro de diálogo **Importar plantilla**:
 - Introduzca un nombre para la nueva plantilla.
 - Haga clic en **Seleccionar un archivo** y, a continuación, seleccione un archivo de plantilla.
 - Seleccione **Servidor**, **Chasis** o **IOA** para indicar el tipo de plantilla.
- 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](#) en la página 68 y [Crear una plantilla desde un dispositivo de referencia](#) en la página 64.
 - 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 > Plantillas**.

- En la lista de plantillas, seleccione la casilla de verificación correspondiente a la plantilla de dispositivo requerida.
- 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 secundario 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 una plantilla de servidor

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.

1. En la página **Plantillas de > cumplimiento**, seleccione la casilla de verificación obligatoria correspondiente y, luego, haga clic en **Editar**.
2. En el cuadro de diálogo **Editar plantilla**:
 - a. En la sección **Información de la plantilla**, edite el nombre y la descripción de la plantilla. 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:
 - La **Vista guiada**: esta vista de atributos muestra solo atributos comunes, agrupados por función. Se muestran atributos de las siguientes categorías:
 - i. En la sección **Configuración del BIOS**, seleccione una de las opciones siguientes:
 - o **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.
 - o **Optimizar según la carga de trabajo**: en el menú desplegable, seleccione perfil de carga de trabajo, seleccione para especificar el tipo de optimización de rendimiento de la carga de trabajo que desea lograr en el perfil.
 - ii. Haga clic en **Arranque** y defina el modo de arranque:
 - o 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.
 - o Si selecciona UEFI como el modo de arranque, arrastre los elementos para establecer la secuencia de arranque de UEFI. Si es necesario, seleccione la casilla de verificación para activar la función Secureboot.
 - iii. Haga clic en **Redes**. Todas las redes asociadas con la plantilla se muestran en las **Interfaces de red**.
 - o 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.
- La **Vista avanzada**: esta vista muestra todos los atributos de plantilla que se pueden cambiar (incluidos los que se muestran en la Vista guiada). Esta vista le permite especificar no solo valores de atributo (como en la Vista guiada), sino que también si cada atributo se incluye o no cuando se implementa la plantilla en un dispositivo de destino.

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

- i. Seleccionada: Indica que todos los atributos del grupo están seleccionados para la implementación.
- ii. Guion: Indica que se seleccionaron algunos de los atributos (pero no todos) para la implementación.

iii. Sin marca: Indica que ninguno de los atributos del grupo está seleccionado para la implementación

NOTA:

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

3. Haga clic en **Siguiente**.

En la sección **Resumen**, se muestran los atributos que editó utilizando los modos Guiado y Avanzado.

4. Esta sección es de solo lectura. Lea la configuración y haga clic en **Finalizar**.

Los atributos de la plantilla actualizada se guardan en la plantilla.

Editar una plantilla de chasis

Es posible editar plantillas de chasis con OpenManage Enterprise.

NOTA: Para editar plantillas de chasis, debe tener privilegios de administrador, o bien de administrador de dispositivos. Para obtener más detalles, consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15.

Para editar una plantilla de chasis:

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

Editar plantilla de IOA

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

Editar las propiedades de red

En la página **Configuración > Plantillas**, puede editar la configuración de la red de las plantillas que contengan los atributos de la NIC correspondientes. Después de seleccionar una plantilla, haga clic en **Editar red** para activar el asistente de edición de red y realice lo siguiente:

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

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

3. En la sección **VLAN** (se aplica solo a los sistemas modulares):

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

NOTA:

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

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

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

d. Realice los cambios en los atributos de **Red sin etiqueta** y la **Red etiquetada** de las NIC asociadas, según sea necesario.

4. Haga clic en **Finalizar** para aplicar los cambios.

Implementar las plantillas de 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](#) en la página 15.

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](#) en la página 64.
- Los dispositivos de destino cumplen con los requisitos especificados en [Requisitos mínimos del sistema para implementar OpenManage Enterprise](#) en la página 19.
- La licencia de OpenManage Enterprise Advanced está instalada en los dispositivos de destino.

PRECAUCIÓN: Asegúrese de que se seleccionen solo los dispositivos apropiados para la implementación. Después de implementar una plantilla de 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 **Plantillas de > configuración**, seleccione la casilla de verificación que corresponde a la plantilla que desea implementar y haga clic en **Implementar plantilla**.

2. En el cuadro de diálogo **Implementar plantilla: <template_name>**, en **Destino**:

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

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

d. Haga clic en **Siguiente**.

3. Si el dispositivo de destino es un servidor, en la sección **Arrancar desde ISO de red**:

- Seleccione la casilla de verificación **Inicio para la imagen ISO de red**.
- 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. Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.
 - d. Haga clic en **Siguiente**.
4. En la sección **IP de administración de iDRAC**, cambie la configuración de IP del dispositivo objetivo, si es necesario, y haga clic en **Siguiente**.

NOTA:

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

5. En la sección **Atributos del objetivo**, los atributos de identidad no virtuales específicos de cada uno de los dispositivos objetivo seleccionados, como los atributos de ubicación y la dirección IP, se pueden modificar antes de la implementación de la plantilla. Cuando se implementa la plantilla, estos atributos del objetivo modificados se implementan solo en los dispositivos específicos. Para cambiar los atributos de identidad no virtuales específicos del dispositivo:
- a. Seleccione un dispositivo objetivo de la lista que muestra los dispositivos objetivo seleccionados anteriormente.
 - b. Expanda las categorías de atributos y, luego, seleccione o anule la selección de los atributos que deben incluirse o excluirse durante la implementación de la plantilla en el dispositivo objetivo.
 - c. Haga clic en **Siguiente**.
6. En la sección **Identidades virtuales**, haga clic en **Identidades reservadas**. Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
- NOTA:** Si las identidades ya están asignadas fuera del dispositivo, una implementación nueva no utilizará esas identidades, a menos que se borren. Para obtener más información, consulte [Grupos de identidades](#) en la página 73
7. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
8. Haga clic en **Finalizar**. Revise el mensaje de advertencia y haga clic en **Sí**. Se crea un trabajo de configuración de dispositivo. Consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105.

Implementar las plantillas de IOA

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](#) en la página 15.

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

- Creó una plantilla de implementación de IOA para la implementación. Consulte [Crear una plantilla desde un dispositivo de referencia](#) en la página 64.
- Los dispositivos de destino cumplen con los requisitos especificados en [Requisitos mínimos del sistema para implementar OpenManage Enterprise](#) en la página 19.
- La versión de firmware del dispositivo de destino es la misma que la de la plantilla IOA.
- Solo se admiten las siguientes implementaciones entre plantillas:

Tabla 13. Implementaciones compatibles entre plantillas

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

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

1. En la lista de plantillas de la página **Configuración > Plantillas**, seleccione la casilla de verificación que corresponde a la plantilla de IOA que desea implementar y haga clic en **Implementar plantilla**.
2. En el cuadro de diálogo **Implementar plantilla: <template_name>**, en **Destino:**

- a. Haga clic en **Seleccionar** y, a continuación, seleccione dispositivos en el cuadro de diálogo **Destino del trabajo**. Consulte [Selección de dispositivos y grupos de dispositivos destino](#).
- b. Haga clic en **Aceptar**.
3. En el cuadro de diálogo **Nombres de host**, puede cambiar el **nombre del host** del dispositivo de IOA de destino. Haga clic en **Siguiente**.
4. En el cuadro de diálogo **Opciones avanzadas**, seleccione el **Modo de vista previa** para simular la implementación, o seleccione **Continuar con la advertencia** para implementar la plantilla y no considerar las advertencias que se presenten. Haga clic en **Siguiente**.
5. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
6. Haga clic en **Finalizar**. Revise el mensaje de advertencia y haga clic en **SÍ**.
Un trabajo de configuración de dispositivo se crea en Trabajos. Consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105.

Clonar plantillas

1. En el menú **OpenManage Enterprise**, en **Configuración**, haga clic en **Plantillas**.
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.

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

Las plantillas de configuración existente en el OpenManage Enterprise se pueden asignar a los servidores y chasis que están en espera de que sean descubiertos. Estas plantillas de configuración se implementan automáticamente en los respectivos dispositivos cuando se hayan descubierto e incorporado.

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

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

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

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

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

- **Crear** plantillas para la implementación automática. Consulte [Crear destinos de implementación automática](#) en la página 70
- **Eliminar** plantillas innecesarias. Consulte [Eliminar destinos de implementación automática](#) en la página 71
- **Exportar** la plantilla de implementación automática a diferentes formatos. Consulte [Exportar detalles del destino de implementación automática a diferentes formatos](#) en la página 72

Crear destinos de implementación automática

 **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](#) en la página 15

Para crear destinos de implementación automática:

1. Haga clic en **OpenManage Enterprise > Configuración > Implementación automática > Crear**.
Aparece el asistente de **Implementación automática de plantilla**.
2. En la página **Información de la plantilla**, seleccione el tipo de plantilla (Servidor o Chasis).

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

Las entradas en el archivo CSV deben tener el siguiente formato: los identificadores se deben incluir en la lista en la primera columna, uno por fila, comenzando desde la segunda fila. Para obtener una plantilla de archivo CSV, haga clic en **Descargar archivo CSV de muestra**.
6. Haga clic en **Siguiente**.
7. En la página **Información de grupo de destino**, especifique un subgrupo en el **Grupo estático**, si está disponible. Para obtener más información sobre el agrupamiento de dispositivos, consulte [Organizar los dispositivos en grupos](#) en la página 36. Los dispositivos de destino se colocarían en el grupo de destino especificado en el momento del descubrimiento
8. Haga clic en **Siguiente**.
9. Si el dispositivo de destino es un servidor, en la página **Arrancar desde ISO de red**:
 - Seleccione la casilla de verificación **Inicio para la imagen ISO de red**.
 - Seleccione **CIFS** o **NFS**.
 - Ingrese la **Ruta ISO** de ubicación en la que se almacenó el archivo de imagen ISO.
 - Ingrese **Dirección IP de recurso compartido, Grupo de trabajo, Nombre de usuario y contraseña**.
 - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.
 - Haga clic en **Siguiente**.
10. En la página **Identidades virtuales**, haga clic en **Identidades reservadas**.
Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
11. En la sección **Atributos del objetivo**, los atributos de identidad no virtuales específicos de cada uno de los dispositivos objetivo seleccionados, como los atributos de ubicación y la dirección IP, se pueden modificar antes de la implementación de la plantilla. Cuando se implementa la plantilla, estos atributos del objetivo modificados se implementan solo en los dispositivos específicos. Para cambiar los atributos de identidad no virtuales específicos del dispositivo:
 - a. Seleccione un dispositivo objetivo de la lista que muestra los dispositivos objetivo seleccionados anteriormente.
 - b. Expanda las categorías de atributos y, luego, seleccione o anule la selección de los atributos que deben incluirse o excluirse durante la implementación de la plantilla en el dispositivo objetivo.
 - c. Haga clic en **Siguiente**.
12. Haga clic en **Finalizar**.
Mensaje de alerta *Es posible que la implementación de una plantilla cause la pérdida de datos y un reinicio del dispositivo. ¿Está seguro de que desea implementar la plantilla?* aparece en la pantalla.
13. Haga clic en **Sí**.
En la página **Implementación automática** se crea y se indica un nuevo destino de implementación automática.

Eliminar destinos de implementación automática

NOTA: Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15

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

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

1. Vaya a la página de implementación automática haciendo clic en **OpenManage Enterprise > Configuración > Implementación automática**.

2. Seleccione los destinos de implementación automática en la lista.
3. **Eliminar** y, a continuación, haga clic en **Sí** para confirmar.
Los destinos de implementación automática que se seleccionan para su eliminación, se eliminan de la página de implementación automática.

Exportar detalles del destino de implementación automática a diferentes formatos

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

Descripción general de la implementación sin estado

Para implementar una plantilla de 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.

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 exclusivos 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.

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:

- Identidades de Ethernet
 - Las identidades de Ethernet definidas por la dirección de control de acceso al medio (MAC). Las direcciones MAC son necesarias para las comunicaciones de Ethernet (LAN).
- Identidades de iSCSI
 - Las identidades definidas por el nombre calificado iSCSI (IQN). Las identidades de IQN son necesarias para admitir el inicio desde SAN por medio del protocolo iSCSI.
- Identidades de Fibre Channel (FC)
 - Las identidades definidas por el nombre de nodo mundial (WWNN) y el nombre de puerto de ámbito mundial (WWPN). UN WWNN identidad está asignado a un nodo (dispositivo) en una red fabric FC y puede ser compartida por algunos o todos los puertos de un dispositivo. UN WWPN identidad está asignada a cada puerto en una red fabric FC y es único para cada puerto. WWNN y el WWPN identidades son necesarios para admitir boot-from-SAN y para acceso a los datos mediante FC y Canal de fibra sobre Ethernet (FCoE) protocolos.
- Identidades de Fibre Channel por Ethernet (FCoE)
 - Identidades que proporcionan una identidad virtual única para las operaciones de FCoE. La dirección MAC y las direcciones de FC (es decir, WWNN y WWPN) definen estas identidades. WWNN y el WWPN identidades son necesarios para admitir boot-from-SAN y para acceso a los datos mediante FC y Canal de fibra sobre Ethernet (FCoE) protocolos.

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

NOTA:

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

Crear grupos de identidades

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

Para crear un grupo de tipos de identidades virtuales:

1. En la página **Configuración**, haga clic en **Grupos de identidades**.

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

NOTA: El grupo de IP del iniciador iSCSI no es compatible con las direcciones IPv6.

6. En la sección **FCoE**:
 - a. Seleccione la casilla de verificación **Incluir identidad de FCoE** para incluir identidades de FCoE.
 - b. Ingrese una dirección MAC de inicio y especifique la cantidad de identidades de FCoE que se debe crear.

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

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

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

Crear grupo de identidades: Fibre Channel

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

Incluir identidad de FC Seleccione la casilla para agregar direcciones de FC al grupo de identidades.

Reparación post (6 octetos) Ingrese la reparación post en uno de los siguientes formatos:

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

La longitud de la reparación post puede tener un máximo de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir identidad FC**.

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

Acciones

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

Crear grupo de identidades: iSCSI

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

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

Incluir direcciones MAC iSCSI Seleccione la casilla para agregar direcciones MAC de iSCSI al grupo de identidades.

Dirección MAC de inicio Ingrese la dirección MAC de inicio del grupo de identidades en uno de los siguientes formatos:

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

La longitud máxima de una dirección MAC es de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.

Número de direcciones MAC de iSCSI Ingrese el número de direcciones MAC de iSCSI. La dirección MAC puede estar entre 1 y 5000. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.

Configurar el iniciador de iSCSI Seleccione esta casilla de verificación para configurar el iniciador de iSCSI. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.

Prefijo IQN Ingrese el prefijo IQN del grupo de identidades de iSCSI. La longitud del prefijo IQN es de un máximo de 200 caracteres. El sistema genera automáticamente el grupo de direcciones de IQN mediante la adición del número generado para el prefijo. Por ejemplo: <IQN Prefix>.<number>

Esta opción se muestra únicamente si se selecciona la casilla de verificación **Configurar el iniciador de iSCSI**.

NOTA: El IQN configurado con grupos de identidades no se implementa en el sistema de destino si el modo de arranque es "BIOS".

NOTA: Si el nombre del iniciador iSCSI se muestra en una línea separada en el campo Grupos de identidad > Uso > IQN de iSCSI, indica que el IQN de iSCSI está activado solo en esa partición de NIC.

Active el grupo de IP del iniciador de iSCSI Seleccione la casilla de verificación para configurar un grupo de identidades del iniciador de iSCSI. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir direcciones MAC de iSCSI**.

Rango de dirección IP Ingrese el rango de dirección IP para el grupo del iniciador de iSCSI en uno de los siguientes formatos:

- A.B.C.D - W.X.Y.Z
- A.B.C.D/E

Máscara de subred Seleccione la dirección de máscara de subred del grupo de iSCSI en el menú desplegable.

Puerta de enlace Ingrese la dirección de la puerta de enlace del grupo de iSCSI.

Primary DNS Server Ingrese la dirección del servidor DNS principal.

Secondary DNS Server Ingrese la dirección del servidor DNS secundario.

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

Acciones

Anterior Muestra la ficha **Ethernet**.

Siguiente Muestra la ficha **FCoE**.

Finalizar Guarda los cambios y muestra la página **Configuración**.

Cancelar Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Crear grupo de identidades: Fibre Channel por Ethernet

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

Incluir identidad de FCoE Seleccione la casilla para incluir las direcciones MAC de FCoE en el grupo de identidades.

Dirección MAC del protocolo FIP Ingrese la dirección MAC de inicio de protocolo de inicialización FCoE (FIP) del grupo de identidades en uno de los siguientes formatos:

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

La longitud máxima de una dirección MAC es de 50 caracteres. Esta opción se muestra únicamente si se selecciona la casilla de verificación **Incluir identidad FCoE**.

Los valores WWPN/WWNN se generan desde la dirección MAC.

Número de identidades FCoE Seleccione el número necesario de identidades FCoE. Las identidades pueden estar entre 1 y 5000.

Acciones

Anterior Muestra la ficha **iSCSI**.

Siguiente Muestra la ficha **Fibre Channel**.

Finalizar Guarda los cambios y muestra la página **Grupos de identidades**.

Cancelar Cierre el asistente del **Crear grupo de identidades** sin guardar los cambios.

Crear grupo de identidades: Ethernet

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

Incluir direcciones virtuales Ethernet Seleccione la casilla para agregar direcciones MAC virtuales al grupo de identidades.

Dirección MAC 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.

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.

Definir redes

1. Seleccione **Configuración > VLAN > Definir**.
2. En el cuadro de diálogo **Definir Red**, ingrese un nombre y una descripción adecuada.
3. Ingrese el ID. de VLAN y, a continuación, seleccione el tipo de red.
Puede seleccionar un tipo de red solamente para el chasis MX7000. Para obtener más información sobre los tipos de red, consulte [Tipos de red](#) en la página 77.
4. Haga clic en **Finalizar**.

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

Tipos de red

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

Tabla 14. Tipos de red

Tipos de red	Descripción
Propósito general (Bronze)	Se utiliza para tráfico de datos de prioridad baja.
Propósito general (Silver)	Se utiliza para tráfico de datos de prioridad estándar o predeterminada
Propósito general (Gold)	Se utiliza para tráfico de datos de prioridad alta

Tabla 14. Tipos de red (continuación)

Tipos de red	Descripción
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: iSCSI	Se utiliza para las VLAN de iSCSI
Almacenamiento: FCoE	Se utiliza para las VLAN de FCoE
Almacenamiento: replicación de datos	Se utiliza para las VLAN que admiten la replicación de datos de almacenamiento; por ejemplo, para la red de área de almacenamiento virtual de VMware (VSAN)
Migración de máquinas virtuales	Se utiliza para las VLAN que admiten vMotion y tecnologías similares
Registro de VMWare FT	Se utiliza para las VLAN compatibles con la tolerancia a errores VMware

Editar o eliminar una red configurada

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

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

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

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

Exportar definiciones de VLAN

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

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

Importar definiciones de red

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

1. Importar definiciones de VLAN desde un archivo

Para importar definiciones de VLAN desde un archivo:

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

NOTA:

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

Tabla 15. Formato de definición VLAN para archivo CSV

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

y

Tabla 16. Formato de definición de VLAN para archivos JSON

```
[{"Name": "VLAN1", "Description": "VLAN with single ID", "VlanMinimum": 1, "VlanMaximum": 1, "Type": 1}, {"Name": "VLAN2 (Range)", "Description": "VLAN with an ID Range", "VlanMinimum": 2, "VlanMaximum": 10, "Type": 2}]
```

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

2. Importar definiciones de VLAN desde un chasis

Para importar definiciones de VLAN desde un chasis MX7000 existente:

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

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

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


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

Administrar perfiles

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

Los siguientes detalles de los perfiles enumerados se muestran en la página **Configuración > Perfiles**:

Tabla 17. Administrar perfiles: definiciones de campos

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

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

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

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

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

Tabla 18. Estados del perfil y operaciones posibles

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

Tabla 18. Estados del perfil y operaciones posibles (continuación)

Estado del perfil	Editar	Asignar objetivo	Anular asignación del objetivo	Volver a implementar	Migrar
Implementado	Sí	No	Sí	Sí	Sí

- Cree perfiles y realice una reserva previa de las identidades virtuales. Consulte [Crear perfiles](#) en la página 81
- Vea detalles del perfil. Consulte [Ver detalles del perfil](#) en la página 81
- Edite ajustes y atributos del perfil. Consulte [Editar un perfil](#) en la página 82
- Asigne un perfil a un dispositivo o a una etiqueta de servicio (a través de la implementación automática). Consulte [Asignar un perfil](#) en la página 82
- Anule la asignación de un perfil desde un dispositivo o una etiqueta de servicio. Consulte [Anular asignación de perfiles](#) en la página 83
- Vuelva a implementar los cambios del perfil en el dispositivo objetivo asociado. Consulte [Volver a implementar perfiles](#) en la página 84
- Migre el perfil de un objetivo (dispositivo o etiqueta de servicio) a otro.
- Elimine perfiles. Consulte [Eliminar perfiles](#) en la página 85
- Exporte y descargue los perfiles de datos en HTML, CSV o PDF. Consulte [Exportar datos de perfiles en formato HTML, CSV o PDF](#) en la página 85

Temas:

- [Crear perfiles](#)
- [Ver detalles del perfil](#)
- [Perfiles: ver red](#)
- [Editar un perfil](#)
- [Asignar un perfil](#)
- [Anular asignación de perfiles](#)
- [Volver a implementar perfiles](#)
- [Migrar un perfil](#)
- [Eliminar perfiles](#)
- [Exportar datos de perfiles en formato HTML, CSV o PDF](#)

Crear perfiles

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

NOTA: Solo los usuarios con privilegios de administrador de dispositivos o de administrador de OpenManage Enterprise pueden realizar las tareas de administración de perfiles.

Para crear un perfil de una plantilla existente realice lo siguiente:

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

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

Ver detalles del perfil

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

1. Seleccione un perfil de la lista de perfiles en la página **Configuraciones > Perfiles**.
2. Haga clic en **Ver** para activar el asistente para ver el perfil.
3. En la página **Detalles** del asistente, se muestra la información de la plantilla de origen, el nombre, la descripción y el objetivo.

4. Haga clic en **Siguiente**. En la página **Arrancar desde ISO de red**, se muestra la ruta de archivo de imagen ISO, la ubicación compartida del archivo de imagen ISO y el valor del tiempo para adjuntar la ISO si el perfil se estableció inicialmente con esa preferencia.


Perfiles: ver red

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

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

Editar un perfil

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

 **NOTA: Solo los usuarios con privilegios de administrador de OpenManage Enterprise pueden realizar estas tareas.**

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

1. Seleccione **Cambiar nombre** y, en el asistente para cambiar el nombre del perfil, edite el nombre del perfil en el cuadro **Nombre**.
2. Seleccione **Editar perfil** para activar el asistente editar el perfil y editar lo siguiente:
 - a. En la página **Detalles**, puede editar el **Nombre** y la **Descripción**. Haga clic en **Siguiente**.
 - b. En la página Arrancar desde ISO de red, seleccione la casilla de verificación **Arrancar desde ISO de red** para especificar la ruta completa de la ISO y la ubicación del recurso compartido, y realice lo siguiente:
 - Seleccione el **Tipo de recurso compartido** como CIFS o NFS.
 - En el cuadro **Ruta de la ISO**, ingrese la ruta completa de la ISO.
 - Proporcione los detalles en los cuadros **Dirección IP de recurso compartido**, **Nombre de usuario** y **Contraseña**.
 - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado al dispositivo objetivo. De forma predeterminada, este valor se configura como cuatro horas.
 - Haga clic en **Siguiente**.
 - c. En la página **IP de administración de iDRAC**, selecciona una de las siguientes opciones:
 - No cambiar los ajustes de IP.
 - Establecer como DHCP.
 - Establecer la IP estática y proporcionar los detalles correspondientes de la IP de administración, la máscara de subred y el gateway.
 - d. En la página de **Atributos del objetivo**, puede seleccionar y editar los atributos del BIOS, del sistema, de la NIC, de la iDRAC y de la identidad virtual del perfil.
 - e. Haga clic en **Finalizar** para guardar los cambios.

Asignar un perfil

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

 **NOTA:**

- **Solo los usuarios de OpenManage Enterprise con privilegios de administrador o administrador de dispositivos pueden realizar esta tarea.**
- **Los atributos existentes, si los hay, del servidor objetivo se sobrescribirán cuando se implemente un perfil en él.**

- Solo los dispositivos que no están asociados con ningún perfil están disponibles para su implementación o una implementación automática.

1. Para **implementar un perfil**:

- Seleccione un perfil sin asignar en la página **Configuración > Perfiles**, haga clic en **Asignar > Implementar** para activar el asistente de implementación de perfiles.
- En la página **Detalles**, se muestra la plantilla fuente, el nombre del perfil y la descripción. Haga clic en **Siguiente**.
- En la página **Objetivo**:
 - Haga clic en **Seleccionar** y, en la lista de dispositivos, seleccione un dispositivo objetivo.
 - Si es necesario reiniciar después de la implementación, seleccione la casilla de verificación **No reiniciar a la fuerza el SO del host si falla el reinicio automático**.
 - Haga clic en **Siguiente**.
- (Opcional) En la página **Arrancar desde ISO de red**, seleccione la casilla de verificación **Arrancar desde ISO de red** y proporcione la ruta de la ISO correspondiente, los detalles de la ubicación del recurso compartido y el valor del tiempo para adjuntar la ISO. Haga clic en **Siguiente**.
- En la página **IP de administración de iDRAC**, seleccione una de las siguientes opciones y proporcione más detalles importantes.
 - No cambiar la configuración de IP.
 - Establecer como DHCP.
 - Establecer IP estática.
- En la página **Atributos de objetivo**, los atributos se muestran en las secciones BIOS, Sistema, NIC y iDRAC. Puede seleccionar, anular la selección o editar los atributos antes de la implementación.
- En la página **Identidades virtuales**, haga clic en **Identidades reservadas**. Se muestran las identidades virtuales asignadas de las tarjetas NIC del dispositivo de destino seleccionado. Para ver todas las identidades asignadas del pool de identidades del dispositivo de destino seleccionado, haga clic en **Ver todos los detalles de NIC**.
- En la página **Programar**, puede elegir **Ejecutar ahora** para implementar el perfil inmediatamente o elegir **Activar programación** y seleccionar una fecha y hora adecuadas para la implementación del perfil.
- Haga clic en **Finalizar**.

NOTA: Si las identidades ya están asignadas fuera del dispositivo, una implementación nueva no utilizará esas identidades, a menos que se borren. Para obtener más información, consulte [Grupos de identidades](#) en la página 73

2. Para **implementar automáticamente un perfil**, siga estos pasos:

NOTA: En el caso de los dispositivos modulares, la comprobación estricta de las definiciones de VLAN está activada de manera predeterminada.

- Seleccione un perfil sin asignar en la página **Configuración > Perfiles**, haga clic en **Asignar > Implementar automáticamente** para activar el asistente de implementación automática.
- En la página **Detalles**, se muestra la plantilla fuente, el nombre y la descripción (si la hay) del perfil. Haga clic en **Siguiente**.
- En la página **Objetivo**, especifique la etiqueta de servicio o el ID del nodo del dispositivo que aún no se ha detectado en el cuadro **Identificador**. Haga clic en **Siguiente**.
- (Opcional) En la página **Arrancar desde ISO de red**, seleccione la casilla de verificación **Arrancar desde ISO de red** a fin de especificar la ruta completa de la ISO y la ubicación del recurso compartido.
 - Seleccione el **Tipo de recurso compartido** como CIFS o NFS.
 - En el cuadro **Ruta de la ISO**, ingrese la ruta completa de la ISO.
 - Proporcione los detalles en los cuadros **Dirección IP de recurso compartido**, **Nombre de usuario** y **Contraseña**.
 - Seleccione las opciones del menú desplegable **Tiempo para adjuntar la ISO** a fin de establecer la cantidad de horas que el archivo ISO de red permanecerá asignado a los dispositivos objetivo. De forma predeterminada, este valor se configura como cuatro horas.
- Haga clic en **Finalizar**.

Anular asignación de perfiles

Al utilizar **Configuración > Perfiles > Anular asignación**, los perfiles implementados o implementados automáticamente se pueden desasociar de sus respectivos objetivos.

Para anular la asignación de perfiles:

1. Seleccione los perfiles de la lista de perfiles en la página **Configuración > Perfil**.
2. Haga clic en **Anular asignación**.

3. Haga clic en **Finalizar** en el cuadro de diálogo de confirmación.

Se anula la asignación de los perfiles seleccionados y se eliminan las identidades de sus respectivos objetivos.

NOTA: En el caso de los dispositivos objetivo implementados, la anulación de la asignación de los perfiles los revertirá a sus identidades asignadas de fábrica.

Volver a implementar perfiles

Para que los cambios en los atributos de un perfil ya implementado surtan efecto en el dispositivo objetivo asociado, se deben volver a implementar. En el caso de los dispositivos modulares, las definiciones de VLAN pueden configurarse durante la reimplementación; sin embargo, la comprobación estricta para que coincida con los atributos de VLAN está deshabilitada.

Para volver a implementar los perfiles, siga estos pasos:

1. En la página **Configuración > Perfiles** seleccione los perfiles que tengan el estado “Implementado” o “Modificado” (🚩) y haga clic en **Volver a implementar**.
2. En la página Opciones de implementación del atributo del Asistente de reimplementación, seleccione una de las siguientes opciones de implementación de atributos y haga clic en **Siguiente**.
 - **Solo atributos modificados:** se utiliza para volver a implementar solo los atributos modificados en el dispositivo objetivo.
 - **Todos los atributos:** se utiliza para volver a implementar todos los atributos, junto con cualquier atributo modificado, en el dispositivo objetivo.
3. En la página Programar, seleccione una de las siguientes opciones:
 - **Ejecutar ahora** para implementar los cambios de inmediato.
 - **Activar programación** y seleccione una fecha y hora para programar la reimplementación.
4. Haga clic en **Finalizar** para continuar.

Cuando se vuelve a implementar un perfil, se ejecuta un trabajo de **Reimplementación de perfiles**. Puede ver el estado del trabajo en la página **Monitorear > Trabajos**.

Migrar un perfil

Un perfil implementado o autoimplementado se puede migrar de la etiqueta de servicio o el dispositivo objetivo existente a otro dispositivo objetivo o etiqueta de servicio idéntico.

Cuando una migración se realiza correctamente, la asignación objetivo del perfil refleja el nuevo objetivo. Si la migración se realiza desde un dispositivo objetivo a una etiqueta de servicio que aún no se ve, el estado del perfil se cambia a “Asignado”.

NOTA:

- **Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol en la página 15.**
- **Migrar perfil cambiará la configuración definida por el perfil (incluidas las identidades virtuales implementadas) de la fuente al objetivo.**
- **Puede forzar la migración de un perfil incluso si no se puede establecer una conexión con el dispositivo fuente. En este caso, el usuario debe asegurarse de que no existan conflictos de identidad virtual.**
- **Los atributos específicos del objetivo verdadero no se reciben del servidor “fuente” como parte de la migración. Debido a esto, los mismos detalles de inventario pueden estar presente en dos servidores después de la migración.**

Para migrar un perfil, siga estos pasos:

1. En la página **Configuración > Perfiles**, seleccione un perfil y haga clic en **Migrar** para activar el asistente de migración de perfiles.
2. En la página Selección:
 - a. En el menú desplegable **Seleccionar perfil fuente**, seleccione el perfil que desea migrar.
 - b. Haga clic en **Seleccionar objetivo** y, en el cuadro de diálogo Objetivo del trabajo, seleccione un dispositivo objetivo y haga clic en **Aceptar**.
 - c. Si es necesario, seleccione la casilla de verificación “Forzar la migración incluso si no se puede establecer una conexión con el dispositivo fuente”.

NOTA: Debe asegurarse de que no existan conflictos de identidad virtual.

- d. Haga clic en **Siguiente**.

3. En la página Programar, seleccione una de las siguientes opciones:
 - a. Seleccione **Actualizar ahora** para migrar la configuración del perfil inmediatamente al objetivo.
 - b. Seleccione una **fecha** y una **hora** para programar la migración.
4. Haga clic en **Finalizar**.

Se crea un trabajo para migrar la configuración del perfil al nuevo dispositivo objetivo. Puede ver el estado del trabajo en la página **Supervisión > Trabajos**.

Eliminar perfiles

Los perfiles "sin asignación" existentes se pueden eliminar de la página **Configuración > Perfiles**:

NOTA:

- **Un perfil asignado o implementado solo se puede eliminar del portal de perfiles si no está asignado.**
- **La eliminación de un perfil no asignado con identidades reservadas devuelve esas identidades al grupo de identidades desde el cual provienen. Se recomienda esperar 10 minutos para usar estas identidades recuperadas para reservas e implementaciones futuras.**

Para eliminar los perfiles sin asignación:

1. Seleccione los perfiles sin asignar en la página Perfiles.
2. Haga clic en **Eliminar** y confirme haciendo clic en **Sí** cuando se le solicite.

Exportar datos de perfiles en formato HTML, CSV o PDF

Siga estos pasos para exportar datos de perfiles como archivos HTML, CSV o PDF.

1. En la página **Configuración > Perfiles** seleccione los perfiles.
2. Haga clic en **Exportar** y, en el cuadro de diálogo Exportar seleccionado, elija una opción (HTML, CSV o PDF).
3. Haga clic en **Finalizar**. Se descargarán los datos de perfiles en el formato seleccionado.

Administración del cumplimiento de la configuración del dispositivo

Seleccione **OpenManage Enterprise > Configuración > Cumplimiento de la configuración** para crear una configuración de base 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](#) en la página 15.

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 de configuración**, puede hacer lo siguiente:

- Crear una línea base de cumplimiento de la configuración. Consulte [Crear la línea base de cumplimiento de una configuración](#) en la página 89.
- 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](#) en la página 87.

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](#) en la página 93.

El informe de Resumen general de cumplimiento muestra los campos siguientes:

- **CUMPLIMIENTO:** El nivel de cumplimiento de resumen de dispositivos conectados a una línea base de cumplimiento de configuración. El estado del dispositivo con menor cumplimiento (por ejemplo, crítico) se indica como el estado de toda la línea base.
- **NOMBRE:** El nombre de la línea base de cumplimiento de configuración.
- **PLANTILLA:** nombre de la plantilla de cumplimiento que utiliza la línea base.
- **HORA DE LA ÚLTIMA EJECUCIÓN:** La fecha y la hora más recientes en la que se ejecutó la línea de base de cumplimiento.

Para ver el informe de cumplimiento de configuración de una línea base, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Ver informe** en el panel derecho.

Utilice la característica del generador de consultas para generar el nivel del dispositivo en cuanto al cumplimiento de la línea base seleccionada. Consulte [Seleccionar los criterios de una consulta](#) en la página 43.

OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos supervisados y su cumplimiento con la línea base de cumplimiento de configuración. Seleccione **OpenManage Enterprise > Monitorear > Informes > Dispositivos por base de línea de cumplimiento de plantilla** y luego haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

Tareas relacionadas

[Crear la línea base de cumplimiento de una configuración](#) en la página 89

[Editar una línea base de cumplimiento de configuración](#) en la página 90

[Eliminar una línea base de cumplimiento de configuración](#) en la página 91

[Administrar plantillas de línea base de cumplimiento](#) en la página 87

[Seleccionar los criterios de una consulta](#) en la página 43

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](#) en la página 86. 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](#) en la página 87.

Seleccione **Configuración > Cumplimiento de la configuración > Administración de plantillas** para 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](#) en la página 87.
 - Mediante un dispositivo de referencia. Consulte [Crear una plantilla de línea base de cumplimiento a partir de un dispositivo de referencia](#) en la página 88.
 - Mediante la importación desde un archivo de plantilla. Consulte [Crear una línea base de cumplimiento mediante la importación desde un archivo](#) en la página 88.
- Editar una plantilla de cumplimiento. Consulte [Editar una plantilla de cumplimiento de línea base](#) en la página 89.
- Clonar una plantilla de cumplimiento. Consulte [Clonar una plantilla de línea base de cumplimiento](#) en la página 88.
- Exportar un informe sobre una plantilla de cumplimiento. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Exportar**. Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50.
- Eliminar una plantilla de cumplimiento. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Eliminar**.

El cumplimiento de configuración es escalable hasta un máximo de 6000 dispositivos. Para administrar eficientemente la actividad de cumplimiento de configuración a gran escala, realice lo siguiente:

- Deshabilite la tarea de inventario de configuración predeterminada que se activa de forma automática y ejecútela manualmente cuando sea necesario.
- Cree líneas de base de cumplimiento con una menor cantidad de dispositivos. Por ejemplo, los 6000 dispositivos deben categorizarse en cuatro líneas de base independientes con 1500 dispositivos cada una.
- No se debe verificar el cumplimiento de todas las líneas de base al mismo tiempo.

i **NOTA:** Cuando edita una plantilla de cumplimiento, el cumplimiento de configuración se activa automáticamente en todas las líneas de base con las que está asociada. Si existe un caso de uso de edición frecuente de plantillas, el entorno de escalación anterior no es compatible y se recomienda asociar un máximo de 100 dispositivos por línea de base para obtener un rendimiento óptimo.

Información relacionada

[Administración del cumplimiento de la configuración del dispositivo](#) en la página 86

[Editar una línea base de cumplimiento de configuración](#) en la página 90

[Eliminar una línea base de cumplimiento de configuración](#) en la página 91

[Crear una plantilla de línea base de cumplimiento a partir de una plantilla de implementación](#) en la página 87

[Editar una plantilla de cumplimiento de línea base](#) en la página 89

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

1. Haga clic en **Configuración > Cumplimiento de la configuración > Administración de plantillas > Crear > Desde la plantilla de implementación**.

2. En el cuadro de diálogo **Clonar plantilla de implementación**, en el menú desplegable **Plantilla**, seleccione una plantilla 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](#) en la página 87

[Clonar una plantilla de línea base de cumplimiento](#) en la página 88

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](#) en la página 114.

1. Haga clic en **Configuración > Cumplimiento de la configuración > Administración de plantillas > Crear > A partir del dispositivo de referencia**.
2. En el cuadro de diálogo **Crear plantilla de cumplimiento**, ingrese un nombre y una descripción para la plantilla de cumplimiento 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](#) en la página 109.
 - 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 de la configuración > Administración de plantillas > Crear > Importar desde el archivo**.
2. En el cuadro de diálogo **Importar plantilla de cumplimiento**, ingrese un nombre para la plantilla de cumplimiento 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 de la configuración > Administración de plantillas**.
2. Seleccione la plantilla de cumplimiento a clonar y, a continuación, haga clic en **Clonar**.
3. En el cuadro de diálogo **Clonar plantilla**, ingrese el nombre de la nueva plantilla.
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](#) en la página 87

[Editar una plantilla de cumplimiento de línea base](#) en la página 89

Editar una plantilla de cumplimiento de línea base

Las plantillas de cumplimiento de normas se pueden editar en la página **Cumplimiento de configuración > Plantillas de cumplimiento**.

NOTA:

- La edición de una plantilla de configuración que ya está asociada a otras líneas de base generará automáticamente un cumplimiento de configuración para todos los dispositivos en todas las líneas de base que utilizan la plantilla.
- La edición de una plantilla de configuración que está vinculada a varias líneas de base con una gran cantidad de dispositivos puede dar lugar a un cierre de sesión por tiempo de espera agotado, ya que la comprobación de cumplimiento de configuración para todos los dispositivos asociados puede tardar varios minutos. Un tiempo de espera agotado de sesión no indica que los cambios realizados en la plantilla de cumplimiento hayan tenido algún problema.
- Cuando edite una plantilla de línea de base en sistemas a gran escala que constan de 1000 dispositivos administrados o un inventario de configuración de un máximo de 6000 dispositivos administrados, asegúrese de que no haya otras operaciones de cumplimiento o inventario de configuración que se ejecuten al mismo tiempo. Además, deshabilite el trabajo de inventario de configuración predeterminado generado por el sistema en la página **Monitorear > trabajos** (establecer fuente como **Generada por el sistema**).
- Se recomienda que asocie un máximo de 1500 dispositivos por línea de base para obtener un rendimiento óptimo.
- Si existe un caso de uso de edición frecuente de plantillas, se recomienda asociar un máximo de 100 dispositivos por línea de base para obtener un rendimiento óptimo.

1. En la página **Plantillas de cumplimiento**, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Editar**.
2. En la página **Detalles de la plantilla**, se indican las propiedades de configuración de la plantilla.
3. Expanda la propiedad que desea editar y, a continuación, ingrese o seleccione datos en los campos.
 - a. Para activar la propiedad, seleccione la casilla de verificación, si no está activada.
4. Haga clic en **Guardar** o **Descartar** para implementar o rechazar los cambios.
La plantilla queda editada y la información actualizada se guarda.

Tareas relacionadas

[Administrar plantillas de línea base de cumplimiento](#) en la página 87

[Clonar una plantilla de línea base de cumplimiento](#) en la página 88


Crear la línea base de cumplimiento de una configuración

OpenManage Enterprise puede asignar 10 bases a un solo dispositivo y comprobar el nivel de cumplimiento de hasta 250 dispositivos a la vez. Para ver la lista de base, haga clic en **OpenManage Enterprise > Configuración > Cumplimiento de la configuración**.

Puede crear una línea base de cumplimiento de configuración mediante:

- El uso de una plantilla de implementación existente. Consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.
- 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](#) en la página 88.
- El uso de una plantilla importada desde un archivo. Consulte [Crear una línea base de cumplimiento mediante la importación desde un archivo](#) en la página 88.

Cuando selecciona una plantilla para la creación de una línea base, también se seleccionan los atributos asociados con las plantillas. Sin embargo, puede editar las propiedades de la línea base. Consulte [Editar una línea base de cumplimiento de configuración](#) en la página 90.

 **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 de la configuración > Crear base**.
2. En el cuadro de diálogo **Crear línea base de cumplimiento**:
 - En la sección **Información de línea base**:
 - a. En el menú desplegable **Plantilla**, seleccione una plantilla de cumplimiento. Para obtener más información sobre las plantillas, consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.
 - b. Ingrese un nombre y una descripción para la línea base de cumplimiento.
 - c. Haga clic en **Siguiente**.
 - En la sección **Destino**:
 - a. Seleccione los dispositivos o grupos de dispositivos. Solo se muestran los dispositivos compatibles. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.

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](#) en la página 86.

NOTA: Siempre que se crea una línea de base de configuración, el dispositivo crea y ejecuta automáticamente un trabajo de inventario de configuración para recopilar el inventario de los dispositivos asociados con la línea de base, ya que sus datos de inventario no están disponibles. Este trabajo de inventario de configuración recién creado tiene el mismo nombre que la línea base para la cual se recopila el inventario. Además, en la página **Cumplimiento de normas en configuración**, se muestra una barra de progreso que indica el progreso del trabajo de inventario junto con la línea de base respectiva.

Información relacionada

[Administración del cumplimiento de la configuración del dispositivo](#) en la página 86

[Eliminar una línea base de cumplimiento de configuración](#) en la página 91

Editar una línea base de cumplimiento de configuración

Puede editar los dispositivos, el nombre y otras propiedades asociadas con una línea base de configuración. Para ver las descripciones de los campos que aparecen en la lista, consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.

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](#) en la página 89. Lea el mensaje de error y sucesos que aparece y lleve a cabo las acciones necesarias. Para obtener más información sobre los mensajes de error y sucesos, consulte la *Guía de referencia de mensajes de error y eventos* que se encuentra disponible en el sitio de asistencia.

1. Seleccione **Configuración > Cumplimiento de la configuración**.
2. En la lista de líneas base de cumplimiento de la configuración, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Editar la línea base de cumplimiento**, actualice la información. Consulte [Crear la línea base de cumplimiento de una configuración](#) en la página 89.

NOTA: Siempre que se edita una línea de base de configuración, se activa automáticamente un trabajo de inventario de configuración para recopilar el inventario de los dispositivos asociados con la línea de base cuyos datos de inventario no están disponibles. Este trabajo de inventario de configuración recién creado tiene el mismo nombre que la línea base para la cual se recopila el inventario. Además, en la página **Cumplimiento de normas en configuración**, se muestra una barra de progreso que indica el progreso del trabajo de inventario junto con la línea de base respectiva.

Tareas relacionadas

[Administrar plantillas de línea base de cumplimiento](#) en la página 87

[Seleccionar los criterios de una consulta](#) en la página 43

Información relacionada

[Administración del cumplimiento de la configuración del dispositivo](#) en la página 86

[Eliminar una línea base de cumplimiento de configuración](#) en la página 91

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 de la configuración**.
2. En la lista de las líneas base de cumplimiento de configuración, seleccione la casilla de verificación correspondiente y, luego, haga clic en **Ver informe**.
3. En la lista de dispositivos que no cumplen, seleccione uno o más dispositivos y, luego, haga clic en **Hacer compatible**.
4. Programe los cambios de configuración para que se ejecuten de inmediato o después y, luego, haga clic en **Finalizar**.

Para aplicar los cambios de configuración después del siguiente reinicio de servidor, puede seleccionar la opción **Aplicar cambios de configuración en los dispositivos en el siguiente reinicio**.

Se ejecuta una nueva tarea de inventario de configuración y el estado de cumplimiento de la línea base se actualiza en la página **Cumplimiento**.

NOTA: En ocasiones, una línea de base con varios dispositivos puede mostrarse como no compatible de forma permanente, debido a que algunos de los valores de atributo no son necesariamente los mismos en todos los destinos. Por ejemplo, los atributos de Control de arranque, como el IQN de destino de iSCSI, la ID de LUN, la WWPN de destino de FCoE, etc., pueden no ser iguales en todos los destinos y pueden causar un incumplimiento permanente de la línea de base.

Eliminar una línea base de cumplimiento de configuración

Puede eliminar el nivel de cumplimiento de la configuración de los dispositivos asociados con una línea base de configuración. Para ver las descripciones de los campos que aparecen en la lista, consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.

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 de la configuración**.
2. En la lista de líneas base de cumplimiento de la configuración, seleccione la casilla de verificación correspondiente y, a continuación, haga clic en **Eliminar**.
3. Cuando se le pregunte si desea o no eliminar, haga clic en **SÍ**.
La línea base de cumplimiento se elimina y la tabla de líneas base **Resumen de cumplimiento general** se actualiza.

Tareas relacionadas

[Crear la línea base de cumplimiento de una configuración](#) en la página 89

[Seleccionar los criterios de una consulta](#) en la página 43

[Administrar plantillas de línea base de cumplimiento](#) en la página 87

[Editar una línea base de cumplimiento de configuración](#) en la página 90

Información relacionada

[Administración del cumplimiento de la configuración del dispositivo](#) en la página 86

Supervisión de alertas de dispositivos

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

- Supervisar alertas por:
 - [Confirmar alertas](#) en la página 94
 - [Ignorar alertas](#) en la página 94
 - [Visualizar las alertas archivadas](#) en la página 95 y [Descargar las alertas archivadas](#) en la página 95
- Crear y administrar directivas de alerta. Consulte [Directivas de alerta](#) en la página 95.
- Ver definiciones de alerta. Consulte [Definiciones de alerta](#) en la página 101.
- Oculte y muestre las alertas confirmadas. Consulte [Personalizar la visualización de alertas](#) en la página 149.
- Exportar todos los datos de alertas o los datos de alertas seleccionados. Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50.

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

i **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](#) en la página 15.

OpenManage Enterprise ofrece un informe incorporado para ver la lista de dispositivos que supervisa OpenManage Enterprise y las alertas generadas para cada dispositivo. Haga clic en **OpenManage Enterprise** > **Supervisión** > **Informes** > **Cuentas de alertas por informe de dispositivos**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

Conceptos relacionados

[Visualizar los registros de alertas](#) en la página 93

Tareas relacionadas

[Eliminar alertas](#) en la página 94

Temas:

- [Visualizar los registros de alertas](#)
- [Confirmar alertas](#)
- [No confirmar alertas](#)
- [Ignorar alertas](#)
- [Eliminar alertas](#)
- [Visualizar las alertas archivadas](#)
- [Descargar las alertas archivadas](#)
- [Directivas de alerta](#)
- [Definiciones de alerta](#)

Visualizar los registros de alertas

Haga clic en **OpenManage Enterprise** > **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.

i **NOTA:** De manera predeterminada, solo se muestran las alertas no confirmadas.

Puede personalizar la lista de alertas utilizando los **Filtros avanzados**, ubicados en la parte superior izquierda de la lista de alertas, o cambiando la **Configuración de visualización de alertas** en la página **Configuración de la aplicación**. Consulte [Personalizar la visualización de alertas](#) en la página 149

i **NOTA:** En OpenManage Enterprise versión 3.2 y posteriores, se realiza un seguimiento del punto de datos de la Última actualización realizada por; sin embargo, no se hacía un seguimiento de esto en las versiones anteriores. Por lo tanto,

tenga en cuenta que si el registro de alertas se refina mediante el campo de filtro avanzado del usuario, no se mostrarán las alertas confirmadas de las versiones anteriores.

- 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 la interfaz gráfica del usuario de OpenManage Enterprise](#) en la página 33.
 - Haga clic en el nombre del dispositivo de hipervínculo en **NOMBRE DE ORIGEN** para ver y configurar las propiedades del dispositivo que generó la alerta. Consulte [Visualización y configuración de dispositivos](#) en la página 50.
- 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, consulte [Visualizar las alertas archivadas](#) en la página 95.

Tareas relacionadas

[Eliminar alertas](#) en la página 94

Información relacionada

[Supervisión de alertas de dispositivos](#) en la página 93

Confirmar alertas

Después de ver una alerta y entender su contenido, puede confirmar que ha leído el mensaje de alerta.

Para confirmar una alerta, realice los siguientes pasos:

Seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **Confirmar**

Una marca de visto aparece en la columna **CONFIRMAR**. Una vez que se confirma una alerta, se rellena el campo **Última actualización realizada por**, ubicado en la sección de detalles de alerta.

No confirmar alertas

Puede anular la confirmación de alertas si las alertas se confirmaron por error.

Para anular la confirmación de alertas, realice las siguientes acciones:

Seleccione la casilla de verificación correspondiente a las alertas y, a continuación, haga clic en el botón **Anular confirmación**. De lo contrario, puede hacer clic en la marca correspondiente a cada alerta para anular la confirmación.

NOTA: El campo Última actualización realizada por en la sección de detalles de alerta conservará el nombre del último usuario que confirmó la alerta.

Ignorar alertas

Si se omite una alerta se crea una directiva de alerta que se activa y se descartan todas las apariciones futuras de dicha alerta. Seleccione la casilla de verificación correspondiente a la alerta y, a continuación, haga clic en **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](#) en la página 94.

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.

- 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](#) en la página 93

Información relacionada

[Supervisión de alertas de dispositivos](#) en la página 93

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 19. 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 en la página 95.

Descargar las alertas archivadas


Las alertas archivadas son el 10% más antiguo de las alertas (5000) que se purgan cuando las alertas superan las 50.000. Estas 5000 alertas más antiguas se eliminan de la tabla, se almacenan en un archivo .CSV y, luego, se archivan. Para descargar el archivo de alertas archivadas:

- 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.
- 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](#) en la página 15.

Directivas de alerta

NOTA: Algunas de las políticas de alerta de las versiones de OpenManage Enterprise anteriores a la versión 3.3.1 no se implementarán después de la actualización. Las políticas de alerta afectadas se deben editar y guardar para que estén activas nuevamente. Consulte [Categorías de alerta después de la reubicación de EEMI](#) en la página 162 para revisar las alertas que se volvieron a categorizar.


 **NOTA:** Las políticas de alerta anteriores no se implementarán después de la actualización hasta que la casilla de verificación Intervalo de tiempo esté activada. Consulte [Editar políticas de alerta en la página 100](#).


Si hace clic en **OpenManage Enterprise > Alertas > Directivas 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](#) en la página 99. 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](#) en la página 156.
 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:** La función de script remoto requiere que el script se encuentre en un servidor Linux remoto al que pueda acceder OpenManage Enterprise. La ejecución del script remoto no se admite en un servidor 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](#) en la página 108. 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](#) en la página 101
- [Inhabilitar políticas de alerta](#) en la página 101
- [Habilitar políticas de alerta](#) en la página 100
- [Editar políticas de alerta](#) en la página 100
- [Crear políticas de alerta](#) en la página 97

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](#) en la página 15.

- Haga clic en **Directivas de alerta > Crear**.
- 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.
 - Para habilitar una directiva de alerta de manera predeterminada, seleccione la casilla de verificación **Habilitar directiva**.
 - Haga clic en **Siguiente**.
- 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:
 - Haga clic en **Siguiente**.
- En la sección **Destino**, agregue los dispositivos o los grupos. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.
 - 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**.
- (Opcional) De forma predeterminada, las políticas de alertas siempre están activas. Para limitar las fechas y la hora en que se aplica la política, puede hacer lo siguiente en la sección **Fecha y hora**:
 - Llenar las fechas Desde y Hasta para seleccionar el **rango de fechas**.
 - Para especificar la hora en que se aplicará la política, seleccione la casilla de verificación **Intervalo de tiempo** y especifique los períodos.
 - Seleccione las casillas de verificación correspondientes a los días en los que se deben ejecutar las políticas de alerta.
 - Haga clic en **Siguiente**.
- En la sección **Gravedad**, seleccione el nivel de gravedad de la alerta para la cual se debe activar esta directiva.
 - Para seleccionar todas las categorías de gravedad, seleccione la casilla de verificación **Todas**.
 - Haga clic en **Siguiente**.
- 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. Los tokens se pueden usar en los campos **Asunto** y **Mensaje**. Consulte [Sustitución del token en secuencias de comandos remotas y política de alerta](#) en la página 163.
 - NOTA:** Acción de correo electrónico para varias alertas de la misma categoría, el ID de mensaje y el contenido se activan solo una vez cada dos minutos para evitar mensajes de alerta redundantes o repetidos en la bandeja de entrada.
 - 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](#) en la página 99.
 - 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**.
 - Controle 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 la página 99.
 - 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](#) en la página 136.
 - **Móvil**: envía notificaciones a los teléfonos móviles registrados con esta versión de OpenManage Enterprise. Consulte [Configuración de OpenManage Mobile](#) en la página 156.
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](#) en la página 95


[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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](#) en la página 100.
 - 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](#) en la página 99.
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](#) en la página 101
- [Inhabilitar políticas de alerta](#) en la página 101
- [Habilitar políticas de alerta](#) en la página 100
- [Editar políticas de alerta](#) en la página 100
- [Crear políticas de alerta](#) en la página 97
- [Administrar registros de auditoría](#) en la página 103

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](#) en la página 29.
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](#) en la página 29.
5. Haga clic en **Aplicar**.
6. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Ejecutar comandos y scripts remotos

Cuando recibe una SNMP trap, puede ejecutar un script en OpenManage Enterprise. Esto establece una política que abre un vale en el sistema de generación de vales de terceros para la administración de alertas. Puede crear y almacenar solo hasta **cuatro** comandos remotos.

1. Haga clic en **Configuración de la aplicación > Ejecución del script**.
2. En la sección **Configuración de comandos remotos**, haga lo siguiente:
 - a. Para agregar un comando remoto, haga clic en **Crear**.
 - b. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - c. Seleccione uno de los siguientes tipos de comando:
 - i. Script

- ii. RACADM
 - iii. Herramienta IPMI
- d. Si selecciona **Script**, haga lo siguiente:
- i. En la casilla **Dirección IP**, ingrese la dirección IP.
 - ii. Seleccione el método de autenticación: **contraseña** o **clave SSH**.
 - iii. Especifique el **Nombre de usuario** y la **Contraseña** o la **clave SSH**.
 - iv. En la casilla **Comando**, escriba los comandos.
 - Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - La sustitución de token en secuencias de comandos es posible. Consulte [Sustitución del token en secuencias de comandos remotas y política de alerta](#) en la página 163
 - v. Haga clic en **Finalizar**.
- e. Si selecciona **RACADM**, haga lo siguiente:
- i. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - iii. Haga clic en **Finalizar**.
- f. Si selecciona **Herramienta IPMI**, haga lo siguiente:
- i. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - iii. Haga clic en **Finalizar**.
3. Para editar la configuración de los comandos remotos, seleccione el comando y haga clic en **Editar**.
4. Para eliminar la configuración de los comandos remotos, seleccione el comando y haga clic en **Eliminar**.

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](#) en la página 97.

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](#) en la página 95

[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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](#) en la página 97.

NOTA: La casilla de verificación **Intervalo de tiempo** está desactivada de manera predeterminada para las políticas de alerta de las versiones de OpenManage Enterprise anteriores a la versión 3.3.1. Después de actualizar, active la opción **Intervalo de tiempo** y actualice los campos para reactivar las políticas.

Información relacionada

[Directivas de alerta](#) en la página 95

[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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](#) en la página 97.

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](#) en la página 95

[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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](#) en la página 95

[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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.

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](#) en la página 50.

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](#) en la página 15.

Si hace clic en **OpenManage Enterprise** y selecciona los elementos que se encuentran en **Monitorear**, 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](#) en la página 123.
- 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 **Monitorear > Registros de auditoría**.

Aparecen los registros de auditoría de las tareas realizadas que OpenManage Enterprise almacena y muestra mediante el dispositivo. Por ejemplo, los intentos de inicio de sesión del usuario, la creación de directivas de alerta y la ejecución de diferentes trabajos.

2. Para ordenar los datos en cualquiera de las columnas, haga clic en el título de la columna.

3. Para buscar información rápidamente sobre un registro de auditoría, haga clic en **Filtros avanzados**.

Los campos que aparecen a continuación funcionan como filtros para buscar datos rápidamente.

4. Ingrese o seleccione datos en los siguientes campos:

- **Gravedad:** seleccione el nivel de gravedad de los datos de registro.
- **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](#) en la página 50.

7. Para exportar los registros de la consola como un archivo .ZIP, haga clic en **Exportar > Exportar registros de la consola**.

NOTA: Actualmente, en lo que respecta a todos los chasis M1000e detectados con una versión de firmware de chasis 5.1x y anteriores, la fecha en la columna HORA DE REGISTRO en Registros de hardware se muestra como 12 de ENE del 2013. Sin embargo, en todas las versiones de chasis VRTX y FX2, aparece la fecha correcta.

Información relacionada

[Reenvío de registros de auditoría a servidores remotos de Syslog](#) en la página 98

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](#) en la página 100.
 - 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](#) en la página 99.
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](#) en la página 101
- [Inhabilitar políticas de alerta](#) en la página 101
- [Habilitar políticas de alerta](#) en la página 100
- [Editar políticas de alerta](#) en la página 100
- [Crear políticas de alerta](#) en la página 97
- [Administrar registros de auditoría](#) en la página 103

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](#) en la página 15.

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](#) en la página 108, [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](#) en la página 50.
- 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**.
- **NOTA:** Solo se puede deshabilitar la ejecución de los trabajos “programados”. Los trabajos que están activos y en el estado “en ejecución” no se pueden desactivar en la mitad del proceso.
- 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](#)
- [Visualizar la información de trabajos individuales](#)
- [Crear un trabajo para hacer parpadear los LED del dispositivo](#)
- [Crear un trabajo para administrar dispositivos de alimentación](#)
- [Crear un trabajo de comando remoto para la administración de dispositivos](#)
- [Crear un trabajo para cambiar el tipo de complemento de la consola virtual](#)
- [Seleccionar dispositivos y grupos de dispositivos de destino](#)

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](#) en la página 106.

Tabla 20. Estado y descripción del trabajo

Estado del trabajo	Descripción
Nuevo	El trabajo se creó, pero no se ejecutado.

Tabla 20. Estado y descripción del trabajo (continuación)

Estado del trabajo	Descripción
En ejecución	El trabajo se activa mediante Ejecutar ahora
Programado	El trabajo está programado para ejecutarse en una fecha u hora posterior.
Completo	El trabajo se ejecutó.
Finalizado con errores	La ejecución del trabajo fue parcialmente correcta y se completó con errores.
Error	La ejecución del trabajo no se realizó correctamente.
Detenido	El usuario interrumpió la ejecución del trabajo.

Un trabajo puede pertenecer a cualquiera de los siguientes tipos:

Tabla 21. Tipos y descripción del trabajo

Tipo de trabajo	Descripción
Estado	Revisa el estado de los dispositivos. Consulte Estados de los dispositivos en la página 39.
Inventario	Crea el informe de inventario de los dispositivos. Consulte Administración del inventario del dispositivo en la página 123.
Configuración de dispositivo	Crea la línea base de cumplimiento de una configuración de dispositivo. Consulte Administración del cumplimiento de la configuración del dispositivo en la página 86.
Report_Task	Crea informes acerca de los dispositivos mediante el uso de campos de datos integrados o personalizados. Consulte Informes en la página 128.
Garantía	Genera datos acerca del estado de garantía de los dispositivos. Consulte Administración de la garantía del dispositivo en la página 126.
Onboarding_Task	Integra los dispositivos detectados. Consulte Incorporación de dispositivos en la página 114.
Detección	Detecta dispositivos. Consulte Detección de dispositivos para la supervisión o administración en la página 110.
Tarea de ejecución de actualización de la consola	Actualizar las versiones de la consola

OpenManage Enterprise ofrece un informe integrado para ver la lista de trabajos programados. Haga clic en **OpenManage Enterprise > Supervisión > Informes > Informe de trabajos programados**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

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](#) en la página 50.

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**:
 - i. En la casilla **Nombre del trabajo**, ingrese el nombre del trabajo.
 - ii. En el menú desplegable **Duración de parpadeo del LED**, seleccione las opciones para hacer parpadear el LED durante un intervalo establecido, para encenderlo o para apagarlo.
 - iii. Haga clic en **Siguiente**.
 - b. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.
 - c. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
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](#) en la página 106.


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**:
 - i. Ingrese el nombre del trabajo en **Nombre del trabajo**.
 - ii. En el menú desplegable **Opciones de alimentación**, seleccione cualquiera de las tareas: **Encender**, **Apagar** o **Realizar el ciclo de apagado y encendido**.
 - iii. Haga clic en **Siguiente**.
 - b. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.
 - c. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
3. Haga clic en **Finalizar**.
El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
4. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
 - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
 - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.
 - Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte [Visualizar la información de trabajos individuales](#) en la página 106.

Crear un trabajo de comando remoto para la administración de dispositivos

Mediante el asistente de trabajos de la línea de comandos, puede crear trabajos de comandos remotos a fin de administrar los dispositivos objetivo de manera remota.

1. Haga clic en **Crear** y, a continuación, seleccione **Comando remoto en dispositivos**.
2. En el cuadro de diálogo **Asistente para trabajos de línea de comandos** en la sección **Opciones**:
 - a. Ingrese el nombre del trabajo en **Nombre del trabajo**.
 - b. En el menú desplegable Interfaz, seleccione una de las interfaces según los dispositivos objetivo que desea administrar:
 - **CLI de IPMI**: para los servidores que no son de Dell y los iDRAC.
 - **CLI de RACADM**: para los iDRAC detectados mediante el protocolo WSMAN.
 - **CLI de SSH**: para servidores Linux detectados mediante el protocolo SSH.
 - c. En el cuadro **Argumentos**, ingrese el comando. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.

 **NOTA:** Los comandos del cuadro **Argumentos** se ejecutan uno a la vez.
 - d. Haga clic en **Siguiente**.
Una marca visto verde junto a **Opciones** indica que se han proporcionado los datos necesarios.
3. En la sección **Destino**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para otro momento. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
5. Haga clic en **Finalizar**.
El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
6. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
 - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
 - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.
 - Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte [Visualizar la información de trabajos individuales](#) en la página 106.

Crear un trabajo para cambiar el tipo de complemento de la consola virtual

Puede cambiar el tipo de complemento de consola virtual a HTML5 en varios dispositivos. La actualización a HTML5 puede dar como resultado una mejor experiencia de navegador. Para actualizar, haga lo siguiente:

1. Haga clic en **OpenManage Enterprise > Supervisión > Trabajos**
2. Haga clic en **Crear** y, a continuación, seleccione **Cambiar complemento de la consola virtual en los dispositivos**.
3. En el cuadro de diálogo **Asistente para cambiar el complemento de la consola virtual**, en la sección **Opciones**:
 - a. Ingrese el nombre del trabajo en **Nombre del trabajo**. De manera predeterminada, el tipo de complemento se muestra como HTML5.
 - b. Haga clic en **Siguiente**.
4. En la sección **Destino del trabajo**, seleccione los dispositivos destino y haga clic en **Siguiente**. Consulte [Seleccionar dispositivos y grupos de dispositivos de destino](#) en la página 109.
 - a. Haga clic en **Siguiente**.
5. En la sección **Programa**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
6. Haga clic en **Finalizar**.
El trabajo se crea y aparece en la lista de trabajos, y se identifica como un estado apropiado en la columna **ESTADO DEL TRABAJO**.
7. Si se programó el trabajo para un momento posterior, pero desea ejecutar el trabajo inmediatamente:
 - En la página Trabajos, seleccione la casilla de verificación correspondiente al trabajo programado.
 - Haga clic en **Ejecutar ahora**. Se ejecuta el trabajo y se actualiza el estado.

- Para ver los datos del trabajo, haga clic en **Ver detalles** en el panel derecho. Consulte [Visualizar la información de trabajos individuales](#) en la página 106.

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](#) en la página 49. Para obtener información acerca de los grupos de dispositivos, consulte [Organizar los dispositivos en grupos](#) en la página 36.

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.

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](#) en la página 15.

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

NOTA: Para admitir la detección con credenciales de dominio, OpenManage Enterprise versión 3.2, y versiones posteriores, utiliza el protocolo OpenSSH en lugar del protocolo WSMAN utilizado en las versiones anteriores. Por lo tanto, todos los dispositivos Hyper-V y Windows descubiertos antes de actualizar el dispositivo deben eliminarse y volver a detectar usando sus credenciales de OpenSSH. Consulte la documentación de Microsoft para habilitar OpenSSH en Hyper-V y Windows.

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](#) en la página 117.
- Crear, ejecutar, editar, eliminar y detener los trabajos de detección de dispositivos.

Tareas relacionadas

[Eliminar un trabajo de detección de dispositivos](#) en la página 122

[Visualizar los detalles del trabajo de detección de dispositivos](#) en la página 116

[Detener un trabajo de detección de dispositivos](#) en la página 116

[Ejecutar un trabajo de detección de dispositivos](#) en la página 116

[Especificar el modo de detección para crear un trabajo de detección de servidores](#) en la página 118

[Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección](#) en la página 118

[Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell](#) en la página 120

[Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP](#) en la página 121

[Especificar el modo de detección para crear VARIOS trabajos de detección](#) en la página 122

[Editar un trabajo de detección de dispositivos](#) en la página 116

Temas:

- [Detectar los servidores automáticamente mediante la función de descubrimiento iniciado por servidor](#)
- [Crear un trabajo de detección de dispositivos](#)
- [Matriz de soporte de protocolos para detectar dispositivos](#)
- [Visualizar los detalles del trabajo de detección de dispositivos](#)
- [Editar un trabajo de detección de dispositivos](#)
- [Ejecutar un trabajo de detección de dispositivos](#)
- [Detener un trabajo de detección de dispositivos](#)
- [Especificar varios dispositivos mediante la importación de datos desde el archivo .csv](#)

- Dispositivos de exclusión global
- Especificar el modo de detección para crear un trabajo de detección de servidores
- Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección
- Especificar el modo de detección para crear un trabajo de detección de chasis
- Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección
- Especificar el modo de detección para crear un trabajo de detección de almacenamiento de Dell
- Especificar el modo de detección para crear un trabajo de detección de conmutadores de red
- Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPS: configuración adicional para los protocolos de detección
- Crear un protocolo de trabajo personalizado de detección de dispositivos para dispositivos SNMP
- Especificar el modo de detección para crear VARIOS trabajos de detección
- Eliminar un trabajo de detección de dispositivos

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

La versión 3.4 de OpenManage Enterprise permite la detección automática de los servidores que tienen la versión de firmware 4.00.00.00 o posterior de iDRAC. El dispositivo se puede configurar para permitir que estos servidores encuentren automáticamente la consola consultando el DNS e iniciar la detección.

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

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

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

1. Agregue la información de configuración de OpenManage Enterprise en el DNS con uno de los siguientes métodos:
 - TUI: mediante la interfaz de TUI, active la opción **Configurar detección iniciada por servidor**. Para obtener más información, consulte [Configurar OpenManage Enterprise con interfaz de usuario de texto](#) en la página 25.
 - Manualmente: agregue los siguientes tres registros al servidor de DNS en la red para los que está configurada la interfaz en el dispositivo. Asegúrese de reemplazar todas las instancias de <domain> con el dominio de DNS correspondiente y el nombre de host del sistema.

- `_dcimprovsvr._tcp.<domain> 3600 PTR ptr.dcimprovsvr._tcp.<domain>`
- `ptr.dcimprovsvr._tcp.<domain> 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence`
- `ptr.dcimprovsvr._tcp.<domain> 3600 SRV 0 0 443 <hostname>.<domain>`

Por ejemplo, consulte la siguiente información mediante nsupdate:

```
1) To create hostname record
>update add omehost.example.com 3600 A XX.XXX.X.XX

2) To add records for Server-initated discovery
>update add _dcimprovsvr._tcp.example.com 3600 PTR ptr.dcimprovsvr._tcp.example.com.

>update add ptr.dcimprovsvr._tcp.example.com 3600 TXT URI=/api/DiscoveryConfigService/Actions/DiscoveryConfigService.SignalNodePresence

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

2. De manera predeterminada, la política de detección-aprobación, en el dispositivo, se establece en Automática y los servidores que establecen contacto con la consola se detectan automáticamente. Para cambiar los ajustes, consulte [Administración de preferencias de consola](#) en la página 147.
3. Una vez que el dispositivo esté configurado como se mencionó en los pasos anteriores, los servidores podrán iniciar el contacto con OpenManage Enterprise consultando el DNS. El dispositivo verifica los servidores después de asegurarse de que el certificado del cliente de los servidores esté firmado por la autoridad de certificación de Dell.
 - NOTA:** Si hay cambios en la dirección IP del servidor o en el certificado SSL, el servidor reiniciará el contacto con OpenManage Enterprise.
4. En la página **Supervisión > Detección iniciada por servidor**, se muestran los servidores que establecen contacto con la consola. También se enumeran los servidores cuyas credenciales se agregaron a la consola, pero que aún no inician el contacto. Se muestran los siguientes estados de los servidores según las condiciones mencionadas anteriormente:
 - Anunciado: el servidor inicia el contacto con la consola; sin embargo, las credenciales del servidor no se agregan a la consola.
 - Credenciales agregadas: se agregan las credenciales del servidor en la consola; sin embargo, el servidor no ha iniciado contacto con la consola.
 - Listo para detectar: se agregan las credenciales del servidor y el servidor ha iniciado contacto.
 - NOTA:** El dispositivo activa un trabajo de detección cada 10 minutos para detectar todos los servidores en el estado “Listo para detectar”. Sin embargo, si la política de detección-aprobación en el dispositivo se configura como “Manual”, el usuario deberá activar manualmente el trabajo de detección para cada servidor. Para obtener más información, consulte [Administración de preferencias de consola](#) en la página 147
 - Trabajo enviado para detección: este estado indica que el trabajo de detección se inició de forma automática o manual para el servidor.
 - Detectado: se detecta el servidor y aparece en la página Todos los dispositivos.

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

1. **Importar:** se utiliza para importar las credenciales de los servidores.
 - a. Haga clic en **Importar**.
 - b. En el asistente de importación de archivos, haga clic en **Cargar archivo de etiquetas de servicio** para navegar y seleccionar el archivo .csv.
Para ver un archivo CSV de muestra de las credenciales del servidor, haga clic en **Descargar archivo CSV de muestra**.
 - c. Haga clic en **Finalizar**.
2. **Detectar:** se utiliza para detectar manualmente los servidores que tienen el estado “Listo para detectar”.
 - a. Seleccione los servidores que se muestran en la página Detección iniciada por servidor que se encuentran en el estado “Listo para detectar”.
 - b. Haga clic en **Detectar**.

Se activa un trabajo de detección para detectar los servidores. La detección posterior de estos servidores se muestra en la página Todos los dispositivos.
3. **Eliminar:** se utiliza para eliminar los servidores enumerados en la página Detección iniciada por servidor.
 - a. Seleccione los servidores en la página Detección iniciada por servidor que ya se detectaron y se enumeran en la página Todos los dispositivos.
 - b. Haga clic en **Eliminar**.

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

 - NOTA:** Las entradas correspondientes a los servidores detectados se depuran automáticamente después de 30 días.
4. **Exportar:** se utiliza para exportar las credenciales del servidor en formato HTML, CSV o PDF.
 - a. Seleccione uno o más servidores en la página Detección iniciada por servidor.
 - b. Haga clic en **Exportar**.
 - c. En el asistente para exportar todo, seleccione cualquiera de los siguientes formatos de archivo: HTML, CSV y PDF.
 - d. Haga clic en **Finalizar**. Se crea un trabajo y los datos se exportan en la ubicación seleccionada.

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](#) en la página 15.

Para detectar un dispositivo:

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

NOTA: Si se detecta una gran cantidad de dispositivos, no se deben crear varios trabajos de detección mediante una dirección IP individual; en su lugar, debe utilizar el rango IP de los dispositivos.

- Para detectar los dispositivos mediante la importación de rangos desde el archivo .csv. Consulte [Especificar varios dispositivos mediante la importación de datos desde el archivo .csv](#) en la página 117.
- Para excluir ciertos dispositivos, quitar dispositivos de exclusión o para ver la lista de dispositivos excluidos detectados, consulte [Dispositivos excluidos globalmente de los resultados de detección](#).

3. En el menú desplegable **Tipo de dispositivo**, para detectar:

- Un servidor, seleccione **SERVIDOR**. Consulte [Especificación del modo de detección para crear un trabajo de detección de servidores](#).
- Un chasis, seleccione **CHASIS**. Consulte [Especificación del modo de detección para crear un trabajo de detección de chasis](#).
- Un dispositivo de almacenamiento Dell EMC o switch de red, seleccione **ALMACENAMIENTO DE DELL** o **SWITCH DE SISTEMA DE RED**. Consulte [Especificación del modo de detección para crear un trabajo de detección de almacenamiento, almacenamiento de Dell y switch de red](#).
- Para detectar los dispositivos usando varios protocolos, seleccione **VARIOS**. Consulte [Especificar el modo de detección para crear VARIOS trabajos de detección](#) en la página 122.

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](#) en la página 161.

8. Seleccione **Habilitar recepción de captura de servidores iDRAC y chasis MX7000 detectados** para permitir que OpenManage Enterprise reciba las capturas entrantes desde los servidores y los chasis MX7000 detectados.

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

9. Seleccione **Establecer cadena de comunidad para el destino trap desde la configuración de la aplicación**. Esta opción está disponible solamente para los servidores iDRAC y chasis MX7000 detectados.

10. Seleccione la casilla de verificación **Enviar por correo electrónico cuando esté terminado** y, a continuación, escriba la dirección de correo electrónico en la cual desea recibir las notificaciones sobre el estado de los trabajos de detección. Si no se configura el correo electrónico, se muestra el vínculo **Ir a la configuración de SMTP**. Haga clic en el vínculo y configure los ajustes de SMTP. Consulte [Configurar alertas de SMTP, SNMP y Syslog](#) en la página 99. Si selecciona esta opción, pero no se configura SMTP, no se muestra el botón **Finalizar** para continuar con la tarea.

11. Haga clic en **Finalizar**. No se muestra el botón Finalizar si los campos son incorrectos o están incompletos. Se crea y ejecuta un trabajo de detección. El estado se muestra en la página **Detalle del trabajo**.

Durante la detección de los dispositivos, la cuenta de usuario que se especifica para el rango de detección se comprueba con respecto a todos los privilegios disponibles activados en un dispositivo remoto. Si la autenticación de usuario se aprueba, el dispositivo automáticamente se incorpora o se puede incorporar posteriormente con diferentes credenciales de usuario. Consulte [Incorporación de dispositivos](#) en la página 114.

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

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

Incorporación de dispositivos

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

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

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

NOTA:


- **Todos los dispositivos que se han incorporado a través de este asistente permanecen incorporados a través de esta cuenta de usuario y la cuenta de usuario de detección no los sustituye durante detecciones futuras de estos dispositivos.**
- **En el caso de los dispositivos ya detectados, si el destino trap de SNMP se establece "manualmente" en iDRAC como OpenManage Enterprise, el dispositivo recibe y procesa las alertas. Sin embargo, el estado administrado del dispositivo que se muestra en la página Todos los dispositivos sigue siendo el mismo que su estado descubierto inicial de "Monitoreado" o "Administrado con alertas".**
- **En la página Todos los dispositivos, se muestra el Estado administrado de todo los chasis incorporados como "administrado", independientemente de las credenciales de función del usuario del chasis que se utilizaron en el momento de la incorporación. Si el chasis se incorporó con las credenciales de un usuario de "solo lectura", es posible que se produzca una falla durante las actividades de actualización realizadas en el chasis. Por lo tanto, se recomienda incorporar un chasis con las credenciales de un administrador de chasis para poder realizar todas las actividades.**
- **Para realizar cualquier tarea en OpenManage Enterprise, debe tener los privilegios necesarios de usuario. Consulte Privilegios de usuario de OpenManage Enterprise basados en el rol en la página 15.**

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](#) en la página 15.
- **Administrado:** el dispositivo se incorporó correctamente y se puede administrar mediante la consola de OpenManage Enterprise.
- **Supervisado:** el dispositivo no tiene opción de administración (como la que se detectó mediante SNMP).
- **Administrado con alertas:** el dispositivo se incorporó correctamente y la consola de OpenManage Enterprise registró correctamente su dirección IP con el dispositivo como destino trap durante la detección.

2. En el panel de trabajo, seleccione la casilla de verificación correspondiente a los dispositivos y haga clic en **Más acciones > Incorporación**.


Asegúrese de seleccionar solamente los tipos de dispositivo en la página Todos los dispositivos que se admiten para la incorporación. Puede buscar dispositivos adecuados en la tabla si hace clic en **Filtros avanzados** y selecciona o escribe datos de estado de incorporación en la casilla de filtro.

-  **NOTA: Todos los dispositivos que se detectan no se admiten para la incorporación y solo iDRAC y CMC son compatibles. Asegúrese de seleccionar la opción de incorporación para el tipo de dispositivo compatible.**

3. En el cuadro de diálogo **Incorporación**, escriba las credenciales de WS-Man: nombre de usuario y contraseña.

4. En la sección **Configuración de conexión**:

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

-  **NOTA: Si el valor de tiempo de espera ingresado es mayor que el tiempo actual de expiración de sesión, se cerrará la sesión de OpenManage Enterprise de forma automática. Sin embargo, si el valor está dentro de la ventana actual de tiempo de expiración de sesión, la sesión se mantiene y no se cierra.**

- c. En la casilla **Puerto**, ingrese el número de puerto que debe utilizar el trabajo para lograr la detección.

- d. Campo opcional. Seleccione **Activar verificación de nombre común (CN)**.
- e. Campo opcional. Seleccione **Habilitar comprobación de entidad de certificación (CA)** y busque el archivo de certificado.

5. Haga clic en **Finalizar**.

i **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.

i **NOTA:** La funcionalidad de los protocolos compatibles para detectar, supervisar y administrar los servidores PowerEdge YX1X con iDRAC6 es limitada. Consulte [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.

Tabla 22. Matriz de compatibilidad de protocolos para detección

Dispositivo/ sistema operativo	Protocolos						
	Administración de servicios web (WS-Man)	Redfish	Protocolo simple de administración de red (SNMP)	Shell seguro (SSH)	Interfaz de administración de plataforma inteligente (IPMI)	ESXi (VMWare)	HTTPS
iDRAC6 o posteriores	Compatible	No compatible	No compatible	No compatible	No compatible	No compatible	No compatible
PowerEdge C *	Compatible	No compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Chasis PowerEdge (CMC)	Compatible	No compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Chasis PowerEdge MX7000	No compatible	Compatible	No compatible	No compatible	No compatible	No compatible	No compatible
Dispositivos de almacenamiento	No compatible	No compatible	Compatible	No compatible	No compatible	No compatible	No compatible
Switch Ethernet	No compatible	No compatible	Compatible	No compatible	No compatible	No compatible	No compatible
ESXi	No compatible	No compatible	No compatible	No compatible	No compatible	Compatible	No compatible
Linux	No compatible	No compatible	No compatible	Compatible	No compatible	No compatible	No compatible
Windows	No compatible	No compatible	No compatible	compatible	No compatible	No compatible	No compatible
Hyper-V	No compatible	No compatible	No compatible	compatible	No compatible	No compatible	No compatible
Servidores que no son Dell	No compatible	No compatible	No compatible	No compatible	Compatible	No compatible	No compatible
PowerVault ME	No compatible	No compatible	No compatible	No compatible	Compatible	No compatible	Compatible

Visualizar los detalles del trabajo de detección de dispositivos

1. Haga clic en **Monitorear > Detección**.
2. Seleccione la fila correspondiente al nombre del trabajo de detección y, a continuación, haga clic en **Ver detalles** en el panel derecho. En la página **Detalles del trabajo** se puede encontrar la información respectiva del trabajo de detección.
3. Para obtener más información acerca de la administración de trabajos, consulte [Utilización de trabajos para el control de dispositivos](#) en la página 105.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

Editar un trabajo de detección de dispositivos

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

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

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

Ejecutar un trabajo de detección de dispositivos

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

Para ejecutar trabajos de detección de dispositivos:

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

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

Detener un trabajo de detección de dispositivos

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

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

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

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

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

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**.
i **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**.
i **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

- i** **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](#) en la página 15.
- i** **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](#) en la página 112.
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.
i **NOTA:** El dispositivo que se excluye de manera global se identifica claramente como "se excluyó de manera global" en la página **Detalles del trabajo**.

Para ver la lista de dispositivos globalmente excluidos, haga clic en:

- **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.

- i** **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.
- i** **NOTA:** Los dispositivos incluidos recientemente en la Lista de exclusión global todavía se ven en la cuadrícula **Todos los dispositivos** hasta el próximo ciclo de detección. Para evitar que se realicen tareas en estos dispositivos, se recomienda

que el usuario marque la casilla de verificación correspondiente a los dispositivos y, a continuación, haga clic en **Excluir** para excluirlos de forma manual de la página **Todos los dispositivos**.

i **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](#).
7. Programe el trabajo de detección. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
8. Haga clic en **Finalizar**.
Un trabajo de detección se crea y se muestra en la lista de trabajos de detección.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

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

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

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

1. Para **Detectar mediante WS-Man/Redfish (iDRAC, servidor o chasis)**
 - a. En la sección **Credenciales**, ingrese **Nombre de usuario** y **Contraseña**.
 - b. En la sección **Configuración de conexión:**
 - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte [Protocolos y puertos admitidos en OpenManage Enterprise](#) en la página 29
 - Seleccione la casilla de verificación **Activar nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
 - Seleccione la casilla de verificación **Habilitar autoridad de certificación (CA)** en caso de ser necesario.
2. Para **Detectar mediante IPMI (no Dell mediante OOB)**

- a. En la sección **Credenciales**, ingrese **Nombre de usuario** y **Contraseña**.
 - b. En la sección **Configuración de conexión**:
 - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - En el cuadro **Key**, ingrese un valor apropiado.
3. Para **Detectar mediante SSH (Linux, Windows, Hyper-V)**
- NOTA:** Solo se admite OpenSSH en Hyper-V y Windows. El protocolo SSH de Cygwin no es compatible.
- a. En la sección **Credenciales**, ingrese **Nombre de usuario** y **Contraseña**.
 - b. En la sección **Configuración de conexión**:
 - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 22 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte [Protocolos y puertos admitidos en OpenManage Enterprise](#) en la página 29
 - Seleccione la casilla de verificación **Comprobar la clave del host conocido** en caso de ser necesario.
 - Seleccione la casilla de verificación **Utilizar opción SUDO** si se prefiere usar cuentas SUDO.

NOTA: Para que las cuentas SUDO funcionen, el archivo `/etc/sudoer` de los servidores se debe configurar para que se pueda utilizar NOPASSWD.
4. Para **Detectar mediante ESXi (VMware)**
- a. En la sección **Credenciales**, ingrese **Nombre de usuario** y **Contraseña**.
 - b. En la sección **Configuración de conexión**:
 - En el cuadro **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - En el cuadro **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - Escriba en el cuadro **Puerto** para editar el número del puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos compatibles, consulte [Protocolos y puertos admitidos en OpenManage Enterprise](#) en la página 29
 - Seleccione la casilla de verificación **Activar nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
 - Seleccione la casilla de verificación **Habilitar autoridad de certificación (CA)** en caso de ser necesario.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

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

1. En el menú desplegable **Tipo de dispositivo**, seleccione **CHASIS**.
En función de su selección, los campos se modifican en **Configuración**.
 2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
 3. En **Configuración**, escriba el nombre de usuario y la contraseña del servidor que se debe detectar.
 4. Escriba el tipo de comunidad.
 5. Para crear plantillas de detección personalizadas cuando se hace clic en **Configuración adicional**, consulte [Creación de un protocolo personalizado de trabajo de detección de dispositivos para los chasis: configuración adicional para los protocolos de detección](#) en la página 120.
- NOTA:** En la actualidad, en todos los chasis M1000e detectados, la fecha en la columna FECHA Y HORA en Registros de hardware es 12 de ENE de 2013 en CMC 5.1x y versiones anteriores. Sin embargo, en todas las versiones de chasis CMC VRTX y FX2, aparece la fecha correcta.
- NOTA:** Cuando se detecta por separado un servidor en un chasis, la información de ranura acerca del servidor no se muestra en la sección Información del chasis. Sin embargo, cuando se detecta mediante un chasis, sí se muestra la información de ranura. Por ejemplo, un servidor MX740c en un chasis MX7000.

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

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

1. Seleccione **Detectar usando WS-Man/Redfish (iDRAC, servidor o chasis)**.
 - NOTA:** Para el chasis, la casilla de verificación **Detectar mediante WS-Man/Redfish** está seleccionada de forma predeterminada. Implica que el chasis se puede detectar utilizando cualquiera de estos dos protocolos. Los chasis M1000e, CMC VRTX y FX2 admiten los comandos de WS-Man. El chasis MX7000 admite el protocolo Redfish.
2. Ingrese el nombre de usuario y la contraseña del chasis que desea detectar.
3. En la sección **Configuración de conexión**:
 - a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - c. Escriba en la casilla **Puerto** para editar el número de puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos, consulte [Protocolos y puertos admitidos en OpenManage Enterprise](#) en la página 29.
 - d. Seleccione la casilla de verificación **Activar verificación de nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
 - e. Seleccione la casilla de verificación **Habilitar comprobación de entidad de certificación (CA)**.
4. Para detectar los módulos de E/S, seleccione la casilla de verificación **Detectar los módulos de E/S con el chasis**.
 - NOTA:** Solo se aplica a los chasis CMC VRTX, M1000e y FX2 (modelos FN2210S, FN410T y FN410S). En el caso del chasis MX7000, los módulos de E/S se detectan automáticamente.
 - NOTA:** Solo los módulos de E/S con modos independientes, PMUX (MUX programable), VLT (Enlace troncal virtual) son visibles. Los modos de conmutador completo o apilados no se detectarán.
 - a. Seleccione **Usar credenciales del chasis** si las credenciales de usuario del agregador M de E/S son las mismas que las del chasis.
 - b. Seleccione **Usar credenciales diferentes** si las credenciales de usuario del agregador M de E/S son diferentes de las credenciales del chasis y realice los siguientes pasos:
 - Ingrese el **Nombre de usuario** y la **Contraseña**.
 - Cambie los valores predeterminados para **Reintentos**, **Tiempo de espera** y **Puerto** si es necesario.
 - Seleccione **Verificar clave de host conocido** para comprobar la identidad del host remoto.
 - Seleccione **Utilizar opción SUDO** si es necesario.
5. Haga clic en **Finalizar**.
6. Realice las tareas en [Crear un trabajo de detección de dispositivos](#) en la página 112.

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

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

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

5. Haga clic en **Ajustes adicionales** para personalizar el protocolo de detección correspondiente. Consulte [Creación de plantillas personalizadas de trabajos de detección de dispositivos para dispositivos SNMP](#) o consulte [Crear un trabajo de detección de dispositivos personalizado para dispositivos de almacenamiento con protocolo HTTPS: configuración adicional para los protocolos de detección](#) en la página 121.
6. Realice las tareas en [Crear un trabajo de detección de dispositivos](#) en la página 112.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

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

1. En el menú desplegable **Tipo de dispositivo**, seleccione **CONMUTADOR DE RED**.
2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
3. En **Configuración**, ingrese la **Versión de SNMP** y el **tipo de comunidad** del dispositivo que se debe detectar.
4. Haga clic en **Ajustes adicionales** para personalizar el protocolo de detección correspondiente. Consulte [Creación de plantillas personalizadas de trabajos de detección de dispositivos para dispositivos SNMP](#)
5. Realice las tareas en [Crear un trabajo de detección de dispositivos](#) en la página 112.


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

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

1. Ingrese el nombre de usuario y la contraseña de PowerVault ME que se detectarán.
2. En la sección **Configuración de conexión**:
 - a. En la casilla **Reintentos**, ingrese la cantidad de intentos repetidos que se deben llevar a cabo para detectar un servidor.
 - b. En la casilla **Tiempo de espera**, ingrese el tiempo que debe transcurrir para que un trabajo se deje de ejecutar.
 - c. Escriba en la casilla **Puerto** para editar el número de puerto. De manera predeterminada, 443 se utiliza para conectarse al dispositivo. Para obtener más información acerca de los números de puertos, consulte [Protocolos y puertos admitidos en OpenManage Enterprise](#) en la página 29.
 - d. Seleccione la casilla de verificación **Activar verificación de nombre común [CN]** si el nombre común del dispositivo es igual al nombre del host usado para acceder a OpenManage Enterprise.
 - e. Seleccione la casilla de verificación **Habilitar comprobación de entidad de certificación (CA)**.
3. Haga clic en **Finalizar**.
4. Realice las tareas en [Crear un trabajo de detección de dispositivos](#) en la página 112.

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

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

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

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

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

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

3. Haga clic en **Finalizar**.
4. Realice las tareas en [Crear un trabajo de detección de dispositivos](#) en la página 112.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

Especificar el modo de detección para crear VARIOS trabajos de detección

1. En el menú desplegable **Tipo**, seleccione **VARIOS** para detectar dispositivos mediante varios protocolos.
2. Ingrese la dirección IP, el nombre de host o el intervalo IP en **Dirección IP/Nombre de host/Intervalo**.
3. Para crear plantillas de detección personalizadas cuando se hace clic en **Configuración adicional**, consulte [Crear protocolo personalizado de trabajo de detección de dispositivos para los servidores: configuración adicional para los protocolos de detección](#) en la página 118.

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

Eliminar un trabajo de detección de dispositivos

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

Para eliminar de un trabajo de detección de dispositivos:

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

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

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

Información relacionada

[Detección de dispositivos para la supervisión o administración](#) en la página 110

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](#) en la página 15.

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

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

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

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

Para obtener información de un trabajo, haga clic en la fila correspondiente al trabajo. El panel derecho muestra los datos del trabajo y los grupos de destino asociados con la tarea de inventario. Para ver información sobre el trabajo, haga clic en **Ver detalles**. La página **Detalles del trabajo** muestra más información. Consulte [Visualizar la información de trabajos individuales](#) en la página 106.

Tareas relacionadas

- [Ejecución de un trabajo de inventario ahora](#) en la página 124
- [Detención de un trabajo de inventario](#) en la página 124
- [Eliminación de un trabajo de inventario](#) en la página 124
- [Creación de un trabajo de inventario](#) en la página 123

Temas:

- [Creación de un trabajo de inventario](#)
- [Ejecución de un trabajo de inventario ahora](#)
- [Detención de un trabajo de inventario](#)
- [Eliminación de un trabajo de inventario](#)
- [Edición de un trabajo de programa de inventario](#)

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](#) en la página 15.

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](#) en la página 36.
4. En la sección **Programación**, ejecute inmediatamente el trabajo o prográmelo para cualquier momento posterior. Consulte [Definiciones de los campos Programar trabajos](#) en la página 161.
5. Se pueden seleccionar las siguientes **Opciones adicionales** mientras se ejecuta el trabajo de inventario:

- Seleccione la casilla de verificación **Recolectar el inventario de la configuración** para generar un inventario de la base de cumplimiento de la configuración.
- Seleccione la casilla de verificación **Recolectar inventario de los controladores** para recolectar información de inventario de controladores del servidor de Windows. Además, para instalar el Recolector de inventario y la Actualización del sistema Dell en el servidor de Windows si estos componentes no están disponibles en el servidor.

NOTA:

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

Para obtener información acerca de las líneas base de cumplimiento de configuración, consulte [Administración del cumplimiento de la configuración del dispositivo](#) en la página 86.

6. Haga clic en **Finalizar**.
7. Se crea el trabajo y se muestra en la cola.
Se crea un trabajo de inventario que se muestra en la lista de trabajos de inventario. La columna **PROGRAMA** especifica si se programó o no el trabajo. Consulte [Ejecución de un trabajo de inventario ahora](#) en la página 124.

Información relacionada

[Administración del inventario del dispositivo](#) en la página 123

Ejecución de un trabajo de inventario ahora

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

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

Información relacionada

[Administración del inventario del dispositivo](#) en la página 123

Detención de un trabajo de inventario

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

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

Información relacionada

[Administración del inventario del dispositivo](#) en la página 123

Eliminación de un trabajo de inventario

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

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

Información relacionada

[Administración del inventario del dispositivo](#) en la página 123

Edición de un trabajo de programa de inventario

1. Haga clic en **Editar**.
2. En el cuadro de diálogo **Programa de inventario**, edite el nombre del trabajo de inventario en **Nombre del trabajo de inventario**. Consulte [Creación de un trabajo de inventario](#) en la página 123.
La tarea del programa de inventario se actualiza y aparece en la tabla.

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](#) en la página 15.

Haga clic en **OpenManage Enterprise > Monitoreo > Garantía** para ver los estados de garantía de todos los dispositivos monitoreados por OpenManage Enterprise.

También puede exportar datos seleccionados o todos los datos a una hoja de Excel para fines estadísticos y de análisis. En la página Garantía se muestran los siguientes detalles:

- **ESTADO** de la garantía

NOTA: El estado de la garantía está determinado por la configuración que seleccione el administrador. Consulte [Administración de la configuración de garantía](#) en la página 150

-  significa **crítico**, que indica que la garantía ha caducado.
-  significa **advertencia**, lo que indica que la garantía se acerca al vencimiento.
-  significa **normal**, lo que indica que la garantía está activa.

- **ETIQUETA DE SERVICIO**

- **MODELO DEL DISPOSITIVO**

- **TIPO DE DISPOSITIVO**

- **TIPO DE GARANTÍA:**

- Inicial: la garantía entregada con la compra de OpenManage Enterprise.
- Extendida: la garantía se extiende, ya que la duración de la garantía inicial expiró.

- **DESCRIPCIÓN DEL NIVEL DE SERVICIO:** indica el Acuerdo de nivel de servicio (SLA) asociado con la garantía del dispositivo.

- **DÍAS RESTANTES:** cantidad de días que faltan para que venza la garantía. Puede establecer los días para recibir una alerta antes de que la garantía caduque. Consulte [Administración de la configuración de garantía](#) en la página 150.

OpenManage Enterprise ofrece un informe incorporado sobre las garantías que vencen en los próximos 30 días. Haga clic en **OpenManage Enterprise > Supervisión > Informes > Garantías que vencen en los próximos 30 días**. Haga clic en **Ejecutar**. Consulte [Ejecutar informes](#) en la página 129.

Para filtrar los datos que se muestran en la tabla, haga clic en **Filtros avanzados**. Consulte acerca de la sección de filtros avanzados [Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise](#) en la página 33.

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](#) en la página 50.

Tareas relacionadas

[Ver y renovar la garantía del dispositivo](#) en la página 126



Temas:

- [Ver y renovar la garantía del dispositivo](#)

Ver y renovar la garantía del dispositivo

Haga clic en **OpenManage Enterprise > Supervisión > Garantía** para obtener una lista de los estados de la garantía de todos los dispositivos supervisados por OpenManage Enterprise, junto con la etiqueta de servicio, el nombre del modelo, el tipo de dispositivo, la garantía asociada y la información del nivel de servicio. Para obtener descripciones sobre campos, consulte [Administración de la garantía del dispositivo](#) en la página 126.

Para ver la información sobre la garantía y para renovar la garantía de un dispositivo:

- Seleccione la casilla de verificación correspondiente al dispositivo. En el panel derecho, se muestra el estado de la garantía y otros detalles importantes del dispositivo, como el código del nivel de servicio, el proveedor de servicios, la fecha de inicio de la garantía, la fecha de término de la garantía, etc.
- Las garantías caducadas se pueden renovar haciendo clic en **Renovación de la garantía de Dell para el dispositivo**. Esta acción lo llevará al sitio de soporte de Dell EMC, en el que podrá administrar la garantía del dispositivo.
- Haga clic en **Actualizar garantía** en la esquina superior derecha para actualizar la tabla Garantía. Los estados de la garantía cambian automáticamente de crítico  a normal  para todos los dispositivos cuyas garantías se renuevan. Cada vez que se hace clic en **Actualizar garantía**, se genera un nuevo registro de alertas de la Garantía del dispositivo con el número total de garantías vencidas en la consola. Para obtener información sobre los registros de alertas, consulte [Ver los registros de alertas](#)
- Para ordenar los datos de la tabla en función de una columna, haga clic en el título de la columna.
- Haga clic en el botón **Filtros avanzados** para personalizar.

Información relacionada

[Administración de la garantía del dispositivo](#) en la página 126

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](#) en la página 15.

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 23. 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/controlador, trabajos programados, resumen de alertas, unidad de disco duro, gabinete modular, NIC, unidad virtual, garantía y licencia.
- Categoría de alertas: alertas semanales

Tareas relacionadas

[Ejecutar informes](#) en la página 129

[Generación de informes y su envío a través de correo electrónico](#) en la página 129

[Editar informes](#) en la página 130

[Eliminar informes](#) en la página 130

Temas:

- [Ejecutar informes](#)
- [Generación de informes y su envío a través de correo electrónico](#)
- [Editar informes](#)
- [Copia de informes](#)
- [Eliminar informes](#)
- [Creación de informes](#)
- [Exportación de informes seleccionados](#)

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](#) en la página 15.

Cuando se ejecuta un informe, se muestran las primeras 20 filas y se pueden paginar los resultados paginados. Para ver todas las filas a la vez, descargue el informe. Para editar este valor, consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50. Los datos que se muestran en la salida no se pueden ordenar, ya que así está definido en la consulta que se utiliza para crear un informe. Para ordenar los datos, edite la consulta de informe o expórtelos a una hoja de Excel. Nota: Se recomienda no ejecutar más de cinco (5) informes a la vez, ya que la generación de informes consume recursos del sistema. Sin embargo, este valor de cinco informes depende de los dispositivos descubiertos, los campos utilizados y la cantidad de tablas que se han unido para generar el informe. Se crea una tarea y se ejecuta cuando se solicita la generación de un informe. Para conocer los privilegios basados en roles necesarios para generar informes, consulte [Creación de informes](#) en la página 130.

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](#) en la página 150.

NOTA: Si va a descargar o ejecutar un informe que ya se generó, y otro usuario intenta eliminar ese informe al mismo tiempo, ambas tareas se llevan a cabo correctamente.

Información relacionada

[Informes](#) en la página 128

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](#) en la página 150.
 - c. Haga clic en **Finalizar**.
El informe se envía por correo electrónico y se registra en los registros de auditoría.

Información relacionada

[Informes](#) en la página 128

Editar informes

Solo se pueden editar los informes creados por el usuario.

1. Seleccione el informe y haga clic en **Editar**.
2. En el cuadro de diálogo **Definición de informe**, edite la configuración. Consulte [Creación de informes](#).
3. Haga clic en **Guardar**.
Se guarda la información actualizada. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

NOTA: Cuando edita un informe personalizado, si la categoría se cambia, los campos asociados también se eliminan.

Información relacionada

[Informes](#) en la página 128

Copia de informes

Solo se pueden copiar los informes creados por el usuario.

1. Seleccione el informe, haga clic en **Más acciones** y, a continuación, haga clic en **Copiar**.
2. En el cuadro de diálogo **Copiar definición de informe**, ingrese un nuevo nombre para el informe copiado.
3. Haga clic en **Guardar**.
Se guarda la información actualizada. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Eliminar informes

Solo se pueden eliminar los informes creados por el usuario. Si se elimina una definición de informe, se elimina también el historial de informes asociados y se detiene cualquier ejecución de un informe que esté utilizando esa definición de informe.

1. En el menú **OpenManage Enterprise**, en **Supervisión**, seleccione **Informes**.
Se muestra una lista de informes disponibles de dispositivos.
2. Seleccione el informe, haga clic en **Más acciones** y, a continuación, haga clic en **Eliminar**.
NOTA: Si va a descargar o ejecutar un informe que ya se generó, y otro usuario intenta eliminar ese informe al mismo tiempo, ambas tareas se llevan a cabo correctamente.
3. En el cuadro de diálogo **Eliminar definición de informe**, cuando se le pregunte si desea eliminar o no el informe, haga clic en **Sí**.
El informe se elimina de la lista de informes y la tabla se actualiza. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Información relacionada

[Informes](#) en la página 128

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](#) en la página 15.

NOTA: Algunas tablas contienen datos específicos del tipo de dispositivo que bloquearán de manera efectiva el informe para ese tipo de dispositivo. La combinación de columnas de tablas específicas de múltiples dispositivos de diferentes tipos (por ejemplo, servidores y chasis) dará como resultado un informe no válido sin resultados.

Si bien los informes integrados tienen definiciones predeterminadas (criterios de filtro) para generar informes, puede personalizar los criterios para crear sus propias definiciones y generar informes personalizados. Los campos o columnas que desee incluir en el informe dependen de la categoría que seleccione. Puede seleccionar solo una categoría a la vez. La disposición de las columnas de un informe se puede modificar mediante la acción de arrastrar y colocar. También:

- Los nombres de los informes deben ser únicos
- La definición del informe debe tener al menos un campo y una categoría
- Para los informes que tienen Dispositivo y Alerta como categorías, el nombre del dispositivo o el grupo de dispositivos debe ser uno de los campos obligatorios

De manera predeterminada, **Dispositivos** se selecciona como categoría, y las columnas de nombre de dispositivo, etiqueta de servicio del dispositivo y modelo del dispositivo se muestran en el panel de trabajo. Si selecciona cualquier otra categoría mientras edita los criterios de un informe, se muestra un mensaje que indica que los campos predeterminados se eliminarán. Cada categoría tiene propiedades predefinidas que se pueden usar como títulos de columnas en las que los datos se filtran según los criterios que usted defina. Ejemplo de tipos de categorías:

- Trabajos: nombre de la tarea, tipo de tarea, estado de la tarea y tarea interna.
- Grupos: estado del grupo, descripción del grupo, tipo de membresía del grupo, nombre del grupo y tipo de grupo.
- Alertas: estado de la alerta, gravedad de la alerta, nombre del catálogo, tipo de alerta, subcategoría de la alerta e información del dispositivo.
- Dispositivos: alerta, catálogo de alerta, ventilador del chasis, software del dispositivo, etc. Estos criterios tienen clasificaciones adicionales según los datos que se pueden filtrar y los informes que se pueden generar.

Tabla 24. Privilegios de acceso basado en roles para generar informes en OpenManage Enterprise

Rol de usuario:	Tareas permitidas en los informes:
Administradores y administradores de dispositivos	Ejecutar, crear, editar, copiar, enviar por correo electrónico, descargar, y exportar
Lectores	Ejecutar, enviar por correo electrónico, exportar, ver y descargar

1. Haga clic en **Informes > Crear**.
2. En el cuadro de diálogo **Definición de informe**:
 - a. Escriba el nombre y la descripción del nuevo informe que desea definir.
 - b. Haga clic en **Siguiente**.
3. En la sección **Generador de informes**:
 - a. En el menú desplegable **Categoría**, seleccione la categoría del informe.
 - Si selecciona Dispositivo como categoría, seleccione el grupo de dispositivos también.
 - Si es necesario, modifique los criterios de filtro. Consulte [Seleccionar los criterios de una consulta](#) en la página 43.
 - b. En la sección **Columnas**, seleccione las casillas de verificación de los campos que deben aparecer como columnas en el informe. Los nombres de los campos seleccionados se muestran en la sección **Orden de columnas**.
 - c. Puede personalizar el informe de las siguientes formas
 - Usando los cuadros **Ordenar por** y **Dirección**.
 - Arrastrando los campos hacia arriba o hacia abajo en la sección **Orden de columnas**.
4. Haga clic en **Finalizar**.
El informe se genera y aparece en la lista de informes. Puede exportar el informe para fines de análisis. Consulte [Exportar todos los datos o aquellos seleccionados](#) en la página 50. Se crea una entrada en el registro de auditoría cada vez que se genera, edita, elimina o copia una definición de informe.

Seleccionar criterios de consulta durante la creación de informes

Defina filtros cuando cree criterios de consulta para:

- Generación de informes personalizados. Consulte [Creación de informes](#) en la página 130.
- Creación de grupos de dispositivos basado en consultas en los GRUPOS PERSONALIZADOS. Consulte [Crear o editar un grupo de dispositivos de consulta](#) en la página 43.

Defina los criterios de consulta mediante dos opciones:

- **Seleccionar consulta existente para copiar**: de manera predeterminada, OpenManage Enterprise proporciona una lista de plantillas de consulta incorporada que puede copiar y crear sus propios criterios de consulta. Cuando se define una consulta, se puede utilizar un máximo de 20 criterios (filtros). Para agregar filtros, debe seleccionar desde el menú desplegable **Seleccionar tipo**.

- **Seleccionar tipo:** cree criterios de consulta desde cero mediante los atributos que se muestran en este menú desplegable. Los elementos en el menú dependen de los dispositivos que supervisa OpenManage Enterprise. Cuando se selecciona un tipo de consulta, se muestran solo operadores adecuados como =, >, < y null según el tipo de consulta. Se recomienda este método para definir criterios de consulta durante la elaboración de informes personalizados.

i **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.

i **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](#) en la página 103.

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.

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](#) en la página 15.

Las herramientas de terceros en su centro de datos pueden generar alertas que son vitales para sus operaciones. Estas alertas se almacenan en archivos de Base de información de administración (MIB) definidos y entendidos por herramientas de los proveedores respectivos. Sin embargo, OpenManage Enterprise también le permite administrar estas MIB, de manera que las MIB que no son de Dell EMC se puedan importar, analizar y utilizar para la administración de dispositivos en OpenManage Enterprise. OpenManage Enterprise admite SMI1 y SMI2. OpenManage Enterprise ofrece archivos de MIB integrados que se pueden utilizar para dispositivos Dell EMC. Estos son MIB solo de lectura y no se pueden editar.

NOTA: OpenManage Enterprise solo administra MIB válidos con capturas.

Puede administrar las MIB de la siguiente manera:

- [Importación de archivos de MIB](#) en la página 133
- [Eliminación de archivos de MIB](#) en la página 135
- [Resolución de tipos de MIB](#) en la página 135

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 25. 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](#) en la página 15**
- **Solo se puede importar un archivo de MIB a la vez.**

1. Haga clic en **MIB > Importar MIB**.
2. En el cuadro de diálogo, **Importar MIB**, en la sección **Cargar archivos de MIB**, haga clic en **Seleccionar archivo** para seleccionar un archivo de MIB.

Si el MIB tiene instrucciones de importación que se resuelven mediante MIB externos, se muestra un mensaje.

- a. Haga clic en **Tipos de resolución**. Resolución de tipos de MIB. Consulte [Eliminación de archivos de MIB](#) en la página 135.
- 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](#) en la página 134.
- El nombre de la captura es de solo lectura. Definido por el dispositivo de terceros.
- Niveles de gravedad de una alerta: Crítica, Aviso, Información y Normal.
- Mensaje de alerta asociado con una alerta.
- El OID de captura es de solo lectura y único.
- "Nuevo" indica que OpenManage Enterprise importa la captura por primera vez. Las excepciones importadas ya se indicaron como "Importadas". "Sobrescribir" indica las capturas cuya definición se vuelve a escribir a causa de una operación de importación.

Para editar los valores predeterminados de las categorías de alerta o el nivel de gravedad de un archivo de MIB, consulte [Edición de capturas de MIB](#) en la página 134. 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](#) en la página 95.

NOTA: Los eventos que se reciben antes de quitar un MIB no se verán afectados por el retiro del MIB asociado. Sin embargo, los eventos que se generen después del retiro tendrán capturas sin formato.

1. En la columna **NOMBRE DE ARCHIVO DE MIB**, expanda, pliegue y seleccione los archivos de MIB.
2. Haga clic en **Eliminar MIB**.
3. En el cuadro de diálogo **Eliminar MIB**, seleccione las casillas de verificación de MIB que se deben eliminar.
4. Haga clic en **Quitar**.
De este modo, se eliminan los archivos de MIB y se actualiza la tabla de MIB.

Resolución de tipos de MIB

1. Importación de archivos de MIB. Consulte [Importación de archivos de MIB](#) en la página 133.
Si el tipo de MIB es sin resolver, en el cuadro de diálogo **Tipos sin resolución** se muestran los tipos de MIB que indican que los tipos de MIB se importarán solo si están resueltos.
2. Haga clic en **Tipos de resolución**.
3. En el cuadro de diálogo **Tipos de resolución**, haga clic en **Seleccionar archivos** y luego seleccione los archivos faltantes.
4. En el cuadro de diálogo **Importar MIB**, haga clic en **Siguiente**. Si todavía hay tipos de MIB faltantes, el cuadro de diálogo **Tipos sin resolución** nuevamente indica los tipos de MIB faltantes. Repita los pasos 1-3.
5. Después de que se resuelvan todos los tipos de MIB sin resolución, haga clic en **Finalizar**. Complete el proceso de importación.
Consulte [Importación de archivos de MIB](#) en la página 133.

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.

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](#) en la página 15.

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

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

- Configurar y administrar los ajustes de red de OpenManage Enterprise, como IPv4, IPv6, tiempo y ajustes de proxy. Consulte [Configuración de red](#).
- Agregar, habilitar, editar y eliminar usuarios. Consulte [Administración de usuarios](#).
- Establecer las propiedades de la condición del dispositivo y de la supervisión del panel. Consulte [Administración de preferencias de la consola](#).
- Administrar políticas de inicio de sesión y bloqueo de usuarios. Consulte [Configuración de propiedades de seguridad de inicio de sesión](#).
- Ver el certificado SSL actual y, a continuación, generar una solicitud de CSR. Consulte [Generación y descarga de la solicitud de firma de certificado](#) en la página 146.
- Configurar correos electrónicos, SNMP y propiedades de Syslog para la administración de alertas. Consulte [Configurar alertas de SMTP, SNMP y Syslog](#) en la página 99.
- Establecer un agente de escucha de SNMP y la configuración de reenvío de capturas. Consulte [Administración de alertas entrantes](#).
- Establecer las credenciales y el tiempo que debe tardar en recibir notificaciones sobre el vencimiento de la garantía. Consulte [Administración de la configuración de garantía](#).
- Establecer las propiedades para comprobar la disponibilidad de versiones actualizadas y, a continuación, actualizar la versión de OpenManage Enterprise. Consulte [Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles](#) en la página 150.
- Establecer las credenciales de usuario para ejecutar un comando remoto mediante RACADM e IPMI. Consulte [Ejecución de comandos y scripts remotos](#).
- Definir y recibir notificaciones de alerta en el teléfono móvil. Consulte [Configuración de OpenManage Mobile](#) en la página 156.

Tareas relacionadas

[Eliminación de servicios de directorio](#) en la página 139

Temas:

- [Configurar los ajustes de la red de OpenManage Enterprise](#)
- [Administración de usuarios de OpenManage Enterprise](#)
- [Activación de usuarios de OpenManage Enterprise](#)
- [Desactivación de usuarios de OpenManage Enterprise](#)
- [Eliminación de usuarios de OpenManage Enterprise](#)
- [Eliminación de servicios de directorio](#)
- [Finalización de sesiones de usuario](#)
- [Privilegios de usuario de OpenManage Enterprise basados en el rol](#)
- [Adición y edición de usuarios de OpenManage Enterprise](#)
- [Edición de propiedades de usuario de OpenManage Enterprise](#)
- [Integración de servicios de directorio en OpenManage Enterprise](#)
- [Establecimiento de las propiedades de seguridad de inicio de sesión](#)
- [Certificados de seguridad](#)
- [Administración de preferencias de consola](#)
- [Personalizar la visualización de alertas](#)

- Administración de alertas entrantes
- Configuración de credenciales de SNMP
- Administración de la configuración de garantía
- Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles
- 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](#) en la página 15.

1. Para ver solo la configuración actual de red de todas las conexiones de red activas de OpenManage Enterprise, como el nombre de dominio DNS, la FQDN y las configuraciones de IPv4 e IPv6, expanda **Configuración actual**.
2. Para configurar los tiempos de espera de la sesión y el número máximo de sesiones para los usuarios de la interfaz web y la API de OpenManage Enterprise, expanda **Configuración del tiempo de espera de inactividad de la sesión** y haga lo siguiente:
 - a. Seleccione la casilla de verificación **Habilitar** para activar el tiempo de espera universal e ingrese el valor del **Tiempo de espera de inactividad (1-1440)**. El valor del tiempo de espera de inactividad se puede establecer entre 1 minuto y 1440 minutos (24 horas). De manera predeterminada, la espera universal aparece atenuada. Cuando se habilita el tiempo de espera universal, se deshabilitan los campos API e Interfaz web.
 - b. Cambie el **Tiempo de espera de inactividad (1-1440)** de la API y los valores de **Número máximo de sesiones (1-100)**. Estos atributos se establecen de forma predeterminada en 30 minutos y 100 minutos respectivamente.
 - c. Cambie el **Tiempo de espera de inactividad (1-1440)** de la interfaz web y los valores de **Número máximo de sesiones (1-100)**. Estos atributos se establecen de forma predeterminada en 30 minutos y 100 minutos respectivamente.
 - d. Haga clic en **Aplicar** para guardar los ajustes o haga clic en **Descartar** para conservar los valores predeterminados.
3. Aparece la hora actual del sistema y el origen, es decir, la zona horaria local o la IP del servidor NTP. Para configurar la zona horaria del sistema, la fecha, la hora y la sincronización del servidor NTP, expanda **Configuración de hora**.
 - a. Seleccione la zona horaria en la lista desplegable.
 - b. Ingrese la fecha o haga clic en el icono de **calendario** para seleccionar la fecha.
 - c. Ingrese la hora con el formato hh:mm:ss.
 - d. Para que se sincronice con un servidor NTP, seleccione la casilla de verificación **Usar NTP** e ingrese la dirección del servidor NTP principal.
Puede configurar hasta tres servidores NTP en OpenManage Enterprise.

NOTA: Las opciones **Fecha** y **Hora** no están disponibles cuando la opción **Usar NTP** está seleccionada.

 - e. Haga clic en **Aplicar**.
 - f. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.
4. Para configurar los ajustes de proxy de OpenManage Enterprise, expanda **Configuración de proxy**.
 - a. Seleccione la casilla de verificación **Activar configuración de proxy HTTP** para configurar el proxy HTTP y luego ingrese la dirección del proxy HTTP y el número de puerto HTTP.
 - b. Seleccione la casilla de verificación **Habilitar autenticación de proxy** para habilitar las credenciales de proxy y, a continuación, ingrese el nombre de usuario y la contraseña.
 - c. Seleccione la casilla de verificación **Ignorar validación del certificado** si el proxy configurado intercepta el tráfico SSL y no usa ningún certificado de confianza de otros fabricantes. Si se usa esta opción, se omitirán las comprobaciones incorporadas del certificado, que se utilizan para la sincronización de la garantía y el catálogo.
 - d. Haga clic en **Aplicar**.
 - e. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Para comprender todas las tareas que puede realizar mediante la característica de Configuración de la aplicación, consulte [Administración de los ajustes del servidor OpenManage Enterprise](#) en la página 136.

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](#) en la página 15.

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).

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

- Ver, agregar, habilitar, editar o eliminar usuarios de OpenManage Enterprise.
 - NOTA:** Cualquier cambio en la función del usuario se aplicará de inmediato y se cerrará la sesión activa de los usuarios afectados.
 - 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](#) en la página 139. Se recomienda utilizar los siguientes caracteres para los nombres de usuario:
 - 0-9
 - A-Z
 - a-z
 - ! # \$ % & () * / ; ? @ [\] ^ _ ` { | } ~ + < = >
 - Se recomiendan los siguientes caracteres para contraseñas:
 - 0-9
 - A-Z
 - a-z
 - ' - ! " # \$ % & () * , . / : ; ? @ [\] ^ _ ` { | } ~ + < = >
- TIPO DE USUARIO:** indica si los usuarios conectados lo hicieron de forma local o remota.
- HABILITADO:** indica con una marca de verificación cuando el usuario está habilitado para realizar tareas de administración de OpenManage Enterprise. Consulte [Activación de usuarios de OpenManage Enterprise](#) en la página 139 y [Desactivación de usuarios de OpenManage Enterprise](#) en la página 139.
- FUNCIÓN:** indica la función del usuario cuando utiliza OpenManage Enterprise. Por ejemplo, administrador y administrador de dispositivos de OpenManage Enterprise. Consulte [Tipos de roles de usuario en OpenManage Enterprise](#) en la página 16.

Referencias relacionadas

[Desactivación de usuarios de OpenManage Enterprise](#) en la página 139

[Activación de usuarios de OpenManage Enterprise](#) en la página 139

Tareas relacionadas

[Eliminación de servicios de directorio](#) en la página 139

[Eliminación de usuarios de OpenManage Enterprise](#) en la página 139

[Finalización de sesiones de usuario](#) en la página 140

Activación de usuarios de OpenManage Enterprise

Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Habilitar**. Si el usuario está habilitado, la marca visto desaparecerá de la celda correspondiente de la columna **HABILITADO**. Si el usuario ya se encuentra habilitado durante la creación del nombre de usuario, el botón **Habilitar** se muestra atenuado.

Tareas relacionadas

[Eliminación de servicios de directorio](#) en la página 139

[Eliminación de usuarios de OpenManage Enterprise](#) en la página 139

[Finalización de sesiones de usuario](#) en la página 140

Información relacionada

[Administración de usuarios de OpenManage Enterprise](#) en la página 138

Desactivación de usuarios de OpenManage Enterprise

Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Deshabilitar**. El usuario está deshabilitado y una marca visto desaparece en la celda correspondiente de la columna **HABILITADO**. Si el usuario está deshabilitado cuando se crea el nombre de usuario, el botón **Deshabilitar** se muestra atenuado.

Tareas relacionadas

[Eliminación de servicios de directorio](#) en la página 139

[Eliminación de usuarios de OpenManage Enterprise](#) en la página 139

[Finalización de sesiones de usuario](#) en la página 140

Información relacionada

[Administración de usuarios de OpenManage Enterprise](#) en la página 138

Eliminación de usuarios de OpenManage Enterprise

1. Seleccione la casilla de verificación correspondiente al nombre de usuario y haga clic en **Eliminar**.
2. Cuando se le solicite, haga clic en **SÍ**.

Referencias relacionadas

[Desactivación de usuarios de OpenManage Enterprise](#) en la página 139

[Activación de usuarios de OpenManage Enterprise](#) en la página 139

Información relacionada

[Administración de usuarios de OpenManage Enterprise](#) en la página 138

Eliminación de servicios de directorio

Seleccione la casilla de verificación correspondiente a los servicios de directorio que se deben eliminar y, a continuación, haga clic en **Eliminar**.

Referencias relacionadas

[Desactivación de usuarios de OpenManage Enterprise](#) en la página 139

[Activación de usuarios de OpenManage Enterprise](#) en la página 139

Información relacionada

[Administración de los ajustes del servidor OpenManage Enterprise](#) en la página 136

[Administración de usuarios de OpenManage Enterprise](#) en la página 138

Finalización de sesiones de usuario

1. Seleccione la casilla de verificación correspondiente al nombre de usuario y, luego, haga clic en **Finalizar**.
2. Cuando se le solicite confirmación, haga clic en **Sí**.
La sesión de usuario seleccionada termina y se cierra la sesión del usuario.

Referencias relacionadas

[Desactivación de usuarios de OpenManage Enterprise](#) en la página 139

[Activación de usuarios de OpenManage Enterprise](#) en la página 139

Información relacionada

[Administración de usuarios de OpenManage Enterprise](#) en la página 138

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. Esta función se conoce como Control de acceso basado en funciones (RBAC). La consola se aplica a una de las funciones por cuenta. Para obtener más información acerca de la administración de usuarios en OpenManage Enterprise, consulte [Administración de usuarios de OpenManage Enterprise](#) en la página 138.

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

Tabla 26. Privilegios de usuario basados en roles en OpenManage Enterprise

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Admin (Administrador)	Administrador de dispositivos	Observador
Ejecutar informes	S	S	S
Ver	S	S	S
Administrar plantillas	S	S	N
Administrar perfiles	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 sistemas operativos	S	S	N
Control de alimentación	S	S	N
Administrar informes	S	S	N
Actualizar inventario	S	S	N

Tabla 26. Privilegios de usuario basados en roles en OpenManage Enterprise (continuación)

Funciones de OpenManage Enterprise	Niveles de usuario para acceder a OpenManage Enterprise		
	Admin (Administrador)	Administrador de dispositivos	Observador
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
Seleccionar destinos para la implementación automática	S	N	N

Referencias relacionadas

[Tipos de roles de usuario en OpenManage Enterprise](#) en la página 16

Tareas relacionadas

[Implementación y administración de OpenManage Enterprise](#) en la página 18

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](#) en la página 15.

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](#) en la página 144.

1. Seleccione **Configuración de la aplicación > Usuarios > Agregar**.
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**
 - **Observador**

Para obtener más información, consulte [Privilegios de usuario de OpenManage Enterprise basados en el rol](#) en la página 15.

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](#) en la página 141.

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.

Integración de servicios de directorio en OpenManage Enterprise

Los servicios de directorio permiten importar grupos de directorios desde AD o LDAP para su uso en la consola. OpenManage Enterprise es compatible con la integración de los siguientes servicios de directorio:

1. Windows Active Directory
2. Windows AD/LDS
3. OpenLDAP
4. PHP con LDAP

Requisitos previos/atributos admitidos para la integración de LDAP

Tabla 27. Requisitos previos/atributos admitidos de OpenManage Enterprise para la integración de LDAP

	Atributo de inicio de sesión del usuario	Atributo de pertenencia a grupos	Requisito de certificado
AD/LDAP	Cn, sAMAccountName	Miembro	<ul style="list-style-type: none">• Debe tener FQSN y está sujeto a las necesidades de certificado de controladora de dominio. El campo SAN puede tener IPv4, IPv6 o FQDN.• Solo se admite el formato de certificado Base64
OpenLDAP	uid, sn	Uniquemember	Solo se admite el formato de certificado PEM
PHP con LDAP	uid	MemberUid	

Requisitos previos de usuario para la integración del servicio de directorio

Debe asegurarse de que se cumplan los siguientes requisitos previos de usuario antes de comenzar con la integración del servicio de directorio:

1. El usuario BindDN y el usuario que se usa para "probar la conexión" deben ser los mismos.
2. Si se proporciona el atributo de inicio de sesión del usuario, se permite solo el valor de nombre de usuario correspondiente asignado al atributo para iniciar sesión en el dispositivo.
3. El usuario que se utiliza para la prueba de conexión debe formar parte de algún grupo no predeterminado de LDAP
4. El atributo de membresía de grupo debe contener el "userDN" o el nombre corto (utilizado para iniciar sesión) del usuario.
5. Cuando MemberUid se utiliza como "atributo de membresía de grupo", se considerará que el nombre de usuario utilizado en el inicio de sesión de dispositivos distingue mayúsculas de minúsculas en algunas configuraciones de LDAP.

6. Cuando el filtro de búsqueda se usa en la configuración de LDAP, el inicio de sesión del usuario no se permite para aquellos usuarios que no forman parte de los criterios de búsqueda mencionados.
7. La búsqueda de grupos funcionará solo si los grupos tienen usuarios asignados en el atributo de membresía de grupo proporcionado.

NOTA: Si OpenManage Enterprise está alojado en una red IPv6, la autenticación SSL en relación con la controladora de dominio que usa el FQDN fallaría si IPv4 se establece como dirección preferida en el DNS. Para evitar este error, realice una de las siguientes acciones:

- DNS debe configurarse para arrojar IPv6 como dirección preferida cuando se consulta con FQDN.
- El certificado DC debe tener IPv6 en el campo SAN.

Para utilizar los servicios de directorio:

- Agregue una conexión de directorios. Consulte [Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio](#) en la página 144.
- Importe grupos de directorio y asigne todos los usuarios en el grupo para un rol específico. Consulte [Importación de grupos de AD y LDAP](#) en la página 143.
- 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](#) en la página 141.

Importación de grupos de AD y LDAP

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

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](#) en la página 144.
 - 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](#) en la página 15.
 - b. Haga clic en **Asignar**.

Los usuarios de un grupo en el servicio de directorio seleccionado se asignan con las funciones del usuario seleccionado.
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.

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

1. Haga clic en **Configuración de la aplicación** > **Usuarios** > **Servicios de directorio** y luego en **Agregar**.
2. En el cuadro de diálogo **Conectarse al servicio de directorio**, de forma predeterminada, se selecciona **AD** para indicar que el tipo de directorio es Active Directory (AD):

 **NOTA:** Para crear un grupo de usuarios de LDAP mediante Servicios de directorio, consulte [Adición o edición de grupos de LDAP que se utilizarán con los Servicios de directorio en la página 144](#).

- a. Ingrese un nombre de su preferencia para el directorio de AD.
 - b. Seleccione el método de búsqueda de las controladoras de dominio:
 - **DNS:** en la casilla **Método**, escriba el nombre del dominio a fin de consultar DNS para las controladoras de dominio.
 - **Manual:** en la casilla **Método**, ingrese la dirección IP o el FQDN de la controladora de dominio. En lo que respecta a varios servidores, se admite un máximo de tres servidores y se debe utilizar una lista separada por comas.
 - c. En la casilla **Dominio del grupo**, ingrese el dominio del grupo como se sugiere en la sintaxis de la información sobre herramientas.
3. En la sección **Opciones avanzadas**:

- a. De manera predeterminada, el número de puerto de la dirección del catálogo global se llena con 3269. Para el acceso a la controladora de dominio, escriba 636 como el número de puerto.

 **NOTA:** Solo se admiten puertos LDAPS.

- b. Escriba la duración del tiempo de espera de red y del tiempo de espera de búsqueda en segundos. La duración del tiempo de espera máximo admitido es de 300 segundos.
- c. Para cargar un certificado SSL, seleccione **Validación del certificado** y haga clic en **Seleccionar un archivo**. El certificado deberá ser un certificado de CA raíz codificado en formato Base64.

Se muestra la pestaña **Probar conexión**.

4. Haga clic en **Probar conexión**.
5. En el cuadro de diálogo, ingrese el **nombre de usuario** y la **contraseña** del dominio al que se debe conectar.

 **NOTA:** El nombre de usuario se debe ingresar en el UPN (**nombredeusuario@dominio**) o en el formato (**dominio\nombre**) de NetBIOS.

6. Haga clic en **Probar conexión**.
En el cuadro de diálogo **Información de servicio de directorio**, se muestra un mensaje para indicar que la conexión es satisfactoria.
7. Haga clic en **Ok**.
8. Haga clic en **Finalizar**.
Se crea y ejecuta un trabajo para agregar el directorio solicitado en la lista de servicios de directorio.

1. En la columna **NOMBRE DE DIRECTORIO**, seleccione el directorio. En el panel derecho se muestran las propiedades del servicio de directorio.
2. Haga clic en **Editar**.
3. En el cuadro de diálogo **Conectarse al servicio de directorio**, edite los datos y haga clic en **Finalizar**. Los datos se actualizan y se guardan.

Adición o edición de grupos de LDAP que se utilizarán con los Servicios de directorio

1. Haga clic en **Configuración de la aplicación** > **Usuarios** > **Servicios de directorio** y luego en **Agregar**.
2. En el cuadro de diálogo **Conectarse al servicio de directorio**, seleccione **LDAP** como el tipo de directorio.

 **NOTA:** Para crear un grupo de usuarios de AD mediante Servicios de directorio, consulte [Adición o edición de grupos de Active Directory para utilizarlos en los Servicios de directorio en la página 144](#).

- a. Ingrese un nombre de su preferencia para el directorio LDAP.
- b. Seleccione el método de búsqueda de las controladoras de dominio:

- **DNS:** en la casilla **Método**, escriba el nombre del dominio a fin de consultar DNS para las controladoras de dominio.
- **Manual:** en la casilla **Método**, ingrese la dirección IP o el FQDN de la controladora de dominio. En lo que respecta a varios servidores, se admite un máximo de tres servidores y se debe utilizar una lista separada por comas.

c. Ingrese el nombre distinguido (DN) de enlace y la contraseña de la carpeta LDAP.

NOTA: No admite el enlace anónimo para LDS de AD.

3. En la sección **Opciones avanzadas:**

a. De manera predeterminada, el número de puerto de LDAP se completa con 636. Para cambiarlo, escriba un número de puerto.

NOTA: Solo se admiten puertos LDAPS.

b. Para que coincida la configuración de LDAP en el servidor, escriba el DN de la base del grupo que desea buscar.

c. Ingrese los **Atributos del usuario** ya configurados en el sistema LDAP. Se recomienda que este nombre sea único dentro del DN base seleccionado. De lo contrario, configure un filtro de búsqueda para garantizar que sea único. Si el DN del usuario no se puede identificar únicamente mediante una búsqueda que combine el atributo y el filtro de búsqueda, falla el inicio de sesión.

NOTA: Antes de integrarlos en los servicios de directorio, los atributos del usuario deben estar configurados en el sistema LDAP que se usa para consultar.

NOTA: Debe ingresar los atributos del usuario como cno sAMAccountName para la configuración de LDS de AD y UID para la configuración de LDAP

d. En el **Atributo de pertenencia a grupos** ingrese el atributo que almacena la información de los grupos y los miembros en el directorio.

e. Escriba la duración del tiempo de espera de red y del tiempo de espera de búsqueda en segundos. La duración del tiempo de espera máximo admitido es de 300 segundos.

f. Para cargar un certificado SSL, seleccione **Validación del certificado** y haga clic en **Seleccionar un archivo** El certificado deberá ser un certificado de CA raíz codificado en formato Base64.

El botón **Probar conexión** está activado.

4. Haga clic en **Probar conexión** y, a continuación, ingrese los parámetros de conexión del usuario de enlace del dominio al que desea conectarse.

NOTA: Mientras se prueba la conexión, asegúrese de que Probar nombre tenga el valor del Atributo de inicio de sesión del usuario especificado previamente.

5. Haga clic en **Probar conexión**.

En el cuadro de diálogo **Información de servicio de directorio**, se muestra un mensaje para indicar que la conexión es satisfactoria.

6. Haga clic en **Aceptar**.

7. Haga clic en **Finalizar**.

Se crea y ejecuta un trabajo para agregar el directorio solicitado en la lista de servicios de directorio.

1. En la columna **NOMBRE DE DIRECTORIO**, seleccione el directorio. En el panel derecho se muestran las propiedades del servicio de directorio.

2. Haga clic en **Editar**.

3. En el cuadro de diálogo **Conectarse al servicio de directorio**, edite los datos y haga clic en **Finalizar**. Los datos se actualizan y se guardan.

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](#) en la página 15.

NOTA: Los usuarios del directorio AD y LDAP pueden importarse y se les puede asignar uno de los roles de OpenManage Enterprise (administrador, administrador de dispositivos o visor).

Haga clic en **OpenManage Enterprise > Configuración de la aplicación > Seguridad** para proteger OpenManage Enterprise especificando la opción **Restringir rango de IP permitido** o **Política de bloqueo de inicio de sesión**.

· Expandir **Restringir rango de IP permitido:**

NOTA: Cuando la opción "Restringir rango de IP permitido" está configurada en un dispositivo, cualquier conexión entrante al dispositivo, como la recepción de alertas, las actualizaciones de firmware y las identidades de red se

bloquea para los dispositivos que no se encuentran dentro del rango determinado. Sin embargo, cualquier conexión que salga del dispositivo funcionará en todos los dispositivos.

1. Para especificar el rango de direcciones IP que deben tener permiso para acceder a OpenManage Enterprise, seleccione la casilla de verificación **Activar rango de IP**.
 2. En la casilla **Dirección de rango IP (CIDR)**, ingrese el rango de direcciones IP.
NOTA: Solo se permite un rango de IP.
 3. Haga clic en **Aplicar**. Para restablecer las propiedades predeterminadas, haga clic en **Descartar**.
NOTA: El botón Aplicar no se activará si se ingresan varios rangos de IP en la casilla Dirección de rango IP (CIDR).
- Expanda **Política de bloqueo de inicio de sesión**:
1. Seleccione la casilla de verificación **Por nombre de usuario** para evitar que con un nombre de usuario específico se inicie sesión en OpenManage Enterprise.
 2. Seleccione la casilla de verificación **Por dirección IP** para evitar que con una dirección IP específica se inicie sesión en OpenManage Enterprise.
 3. En la casilla **Conteo de fallas de bloqueo**, ingrese la cantidad de intentos incorrectos después de los cuales OpenManage Enterprise debe impedir que el usuario vuelva a intentar iniciar sesión. De manera predeterminada, 3 intentos.
 4. En la casilla **Ventana de falla de bloqueo**, ingrese el tiempo durante el cual OpenManage Enterprise debe mostrar información acerca de un intento fallido.
 5. En la casilla **Tiempo de espera de bloqueo**, ingrese el tiempo durante el cual se impide al usuario realizar cualquier intento de inicio de sesión después de varios intentos incorrectos.
 6. Haga clic en **Aplicar**. Para restablecer la configuración a los atributos predeterminados, haga clic en **Descartar**.

Referencias relacionadas

[Certificados de seguridad](#) en la página 146

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 en la página 15.

Para generar una solicitud de firma de certificado (CSR), consulte [Generación y descarga de la solicitud de firma de certificado](#) en la página 146.

Información relacionada

[Establecimiento de las propiedades de seguridad de inicio de sesión](#) en la página 145

Generación y descarga de la solicitud de firma de certificado

Para generar una solicitud de firma de certificado (CSR) para su dispositivo y, a continuación, solicitar un certificado SSL:

NOTA: Solo debe generar la CSR en el dispositivo OpenManage Enterprise.

1. Haga clic en **Generar una solicitud de firma de certificado**.
2. En el cuadro de diálogo **Generar solicitud de firma de certificado**, ingrese información en los campos.
3. Haga clic en **Generar**.
Una CSR se crea y se muestra en el cuadro de diálogo **Solicitud de firma de certificado**. Una copia de la CSR también se envía a la dirección de correo electrónico que se proporciona en la solicitud.
4. En el cuadro de diálogo **Solicitud de firma de certificado**, copie los datos de la CSR y envíela a la autoridad emisora de certificados (CA) mientras se solicita un certificado SSL.
 - Para descargar la CSR, haga clic en **Descargar solicitud de firma de certificado**.
 - Haga clic en **Finalizar**.

Asignar un certificado de servidor web a OpenManage Enterprise mediante los servicios de certificados de Microsoft

1. Generar y descargar la solicitud de firma de certificado (CSR) en OpenManage Enterprise. Consulte [Generación y descarga de la solicitud de firma de certificado](#) en la página 146
2. Abra una sesión web en el servidor de certificación (<https://x.x.x.x/certsrv>) y haga clic en el enlace **Solicitar un certificado**.
3. En la página Solicitar un certificado, haga clic en el enlace **Enviar una solicitud avanzada de certificado**.
4. En la página Solicitud avanzada de certificado, haga clic en el enlace **Enviar una solicitud de certificado mediante un archivo CMC o PKCS#10 codificado de base 64 o enviar una solicitud de renovación mediante un archivo PKCS#7 codificado de base 64**.
5. En la página Enviar una solicitud de certificado o de renovación, realice lo siguiente:
 - a. En el campo **Solicitud de certificado codificado de base 64 (archivo CMC, PKCS#10 o PKCS#7)**, copie y pegue todo el contenido de la CSR descargada.
 - b. En **Plantilla de certificado**, seleccione **Servidor web**.
 - c. Haga clic en **Enviar** para emitir un certificado.
6. En la página Certificado emitido, seleccione la opción **Codificado de base 64** y, luego, haga clic en el enlace **Descargar certificado** para descargar el certificado.
7. Para cargar el certificado en OpenManage, vaya a la página **Configuración de aplicación > Seguridad > Certificados** y, luego, hacer clic en **Cargar**.

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](#) en la página 15.

Si hace clic en **OpenManage Enterprise > Configuración de la aplicación > Preferencias de la consola**, puede establecer las propiedades predeterminadas de la interfaz gráfica de usuario de OpenManage Enterprise. Por ejemplo, la hora predeterminada después de la cual la condición de un dispositivo se comprueba y actualiza automáticamente en el panel, y se usa la configuración preferida para detectar un dispositivo. Las siguientes opciones se encuentran disponibles:

1. **Ajustes de informes:** para establecer el número máximo de filas que se pueden ver en los informes de OpenManage Enterprise:
 - a. Expanda la **Configuración del informe**.
 - b. Ingrese un número en la casilla **Límite de filas de informes**. Cantidad máxima de filas permitidas = 2 000 000 000.
 - c. Haga clic en **Aplicar**. Se ejecuta una tarea y se aplica el valor.
2. **Estado del dispositivo:** para establecer la hora después de la cual el estado de los dispositivos se debe supervisar y actualizar automáticamente en el panel de OpenManage Enterprise:
 - a. Expanda **Condición de los dispositivos**.
 - b. Ingrese la frecuencia con que se debe registrar la condición de los dispositivos y almacenar los datos.
 - c. Seleccione:
 - **Última condición conocida:** muestra la última condición registrada de los dispositivos cuando se pierde la conexión de alimentación.
 - **Desconocido:** mostrar la última condición registrada del dispositivo cuando el estado del dispositivo se mueve a "desconocido". Un dispositivo se convierte en desconocido para OpenManage Enterprise cuando se pierde la conexión con iDRAC y el dispositivo ya no se supervisa en OpenManage Enterprise.
 - d. Haga clic en **Aplicar** para guardar los cambios realizados en la configuración o haga clic en **Descartar** para conservar la configuración predeterminada.
3. **Ajuste de la detección:** expanda Ajuste de la detección para establecer la nomenclatura de dispositivos que utiliza OpenManage Enterprise para identificar las iDRAC detectadas y otros dispositivos mediante los ajustes **Nombres generales de dispositivos y Nombres de dispositivos del servidor**.

NOTA: Las opciones de nombres de dispositivos en **Nombres generales de dispositivos y Nombres de dispositivos del servidor** son independientes una de la otra y no inciden en la otra.

 - a. **Nombres generales de dispositivos** se aplica a todos los dispositivos detectados que no sean de iDRAC. Seleccione uno de los siguientes modos de nombre:
 - **DNS** para utilizar el nombre DNS.

- **Instrumentación (NetBIOS)** para utilizar el nombre de NetBIOS.

i **NOTA:**

- **El ajuste predeterminado de Nombres generales de dispositivos es DNS.**
- **Si alguno de los dispositivos detectados no tiene el nombre DNS o el nombre de NetBIOS para cumplir el ajuste, entonces el dispositivo identifica aquellos dispositivos por sus direcciones IP.**
- **Cuando se selecciona la opción Instrumentación (NetBIOS) en Nombres generales de dispositivos, en el caso de los dispositivos de chasis, se muestra el nombre del chasis como la entrada del nombre del dispositivo en la página Todos los dispositivos.**

- b. **Nombres de dispositivos del servidor** solo se aplica a los iDRAC. Seleccione uno de los siguientes modos de nombres para las iDRAC detectadas:

- **Nombre de host del iDRAC** para usar el nombre de host del iDRAC.
- **Host del sistema** para utilizar el nombre de host del sistema.

i **NOTA:**

- **La preferencia de nombres predeterminados de los dispositivos iDRAC es el Nombre de host del sistema.**
- **Si alguno de los iDRAC no tiene el nombre de host del iDRAC o el nombre de host del sistema para cumplir el ajuste, entonces el dispositivo identifica los iDRAC mediante sus direcciones IP.**

- c. Para especificar los nombres de host de dispositivos que no son válidos y las direcciones MAC comunes, expanda la **Configuración avanzada**.

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

- d. Haga clic en **Aplicar** para guardar los cambios en la configuración o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.

4. **Detección iniciada por servidor.** Seleccione una de las siguientes políticas de aprobación de detecciones:

- **Automático:** para permitir que la consola detecte automáticamente los servidores con la versión del firmware 4.00.00.00 de la iDRAC que se encuentren en la misma red que la consola.
- **Manual:** para que el usuario detecte manualmente los servidores.
- Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.

5. **Preferencias de incorporación de MX7000:** especifique uno de los siguientes comportamientos de reenvío de alertas en los chasis MX7000 cuando estos se incorporen:

- Recibir todas las alertas
- Recibir solo las alertas de categoría de “chasis”

6. **Ajustes de SMB:** para seleccionar una versión de Server Message Block (SMB) que se debe usar para la comunicación de red:

- **Desactivar V1:** se desactiva SMBv1. Esta es la selección predeterminada en el dispositivo.
- **Activar V1:** para activar SMBv1.

i **NOTA:** Asegúrese de habilitar SMBv1 en la Configuración de SMB antes de que comience cualquier tarea que necesite comunicación con algún chasis o los servidores PowerEdge YX2X o YX3X que cuenten con la versión 2.50.50.50 de iDRAC o versiones anteriores. Consulte [Administración de preferencias de consola](#) en la página 147 y [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#) en la página 165 para obtener más información.

7. **Ajustes del remitente de correo electrónico:** para establecer la dirección del usuario que envía un mensaje de correo electrónico:

- Ingrese una dirección de correo electrónico en el cuadro **ID de correo electrónico del remitente**.
- Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.

8. **Formato de reenvío de trap:** para establecer el formato de reenvío de trap:

- Seleccione una de las siguientes opciones
 - **Formato original (válido solo para trap de SNMP):** para conservar los datos de trap tal como están.
 - **Normalizado (válido para todos los eventos):** se utiliza para normalizar los datos de captura. Cuando el formato de reenvío de capturas se configura en “Normalizado”, el agente receptor, como el registro del sistema, recibe una etiqueta que contiene la dirección IP del dispositivo desde la cual se reenvió la alerta.

- b. Haga clic en **Aplicar** para guardar los cambios o haga clic en **Descartar** para restablecer la configuración a los atributos predeterminados.
9. **Configuración de recopilación de métricas:** para establecer la frecuencia de mantenimiento y depuración de los datos de la extensión de PowerManager, realice lo siguiente:
- En el cuadro **Intervalo de mantenimiento de datos**, ingrese, en minutos, la frecuencia de las operaciones de mantenimiento de datos.
 - En el cuadro **Intervalo de depuración de datos**, ingrese la frecuencia con la que desea eliminar los datos de PowerManager. Puede ingresar valores comprendidos entre 30 y 365 días.

Personalizar la visualización de alertas

1. Haga clic en **OpenManage Enterprise > Configuración de la aplicación>Alertas** y expanda **Configuración de visualización de alertas**.
2. Seleccione una de las siguientes opciones:
 - a. **Todas:** para habilitar la visualización de alertas confirmadas y no confirmadas.
 - b. **No confirmadas:** para habilitar la visualización solo de alertas no confirmadas.

NOTA: De manera predeterminada, la Configuración de la visualización de alertas está definida en **No confirmadas**.

- c. **Confirmadas:** para habilitar la visualización solo de alertas confirmadas.
3. Haga clic en **Aplicar**.

Los cambios en la configuración de la visualización de alertas tendrán efecto en las siguientes páginas de OpenManage Enterprise:

- En la esquina superior derecha de todas las páginas de OpenManage Enterprise. Consulte [Descripción general de la interfaz gráfica del usuario de OpenManage Enterprise](#) en la página 33.
- En la página Panel. Consulte [Supervisión de dispositivos mediante el tablero de OpenManage Enterprise](#) en la página 35.
- En la página Dispositivos. Consulte [Gráfico de anillo](#) en la página 38.
- En la tabla **Registro de alertas** de la página Alertas. Consulte [Visualizar los registros de alertas](#) en la página 93.

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](#) en la página 15.

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 el dispositivo, es posible que deba volver a configurar los ajustes mediante el nombre de usuario, una frase de contraseña de autenticación y una frase

de contraseña de privacidad para seguir recibiendo las alertas. Si el problema persiste, reinicie los servicios mediante la interfaz de usuario de texto (TUI).

- 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

La **Configuración de la garantía** determina la visualización de las estadísticas de la garantía por parte de OpenManage Enterprise en el widget de Alerta de la página de inicio, el cuadro de mandos en todas las páginas, la página Garantía y los informes.

Para cambiar la configuración de la garantía, realice los siguientes pasos:

1. Haga clic en **OpenManage Enterprise > Configuración de la aplicación > Garantía**
2. Haga clic en **Configuración de la garantía** para activar el cuadro de diálogo.
3. En el cuadro **Mostrar advertencia si las garantías expiran en los próximos**, ingrese el número de días. Puede ingresar un valor entre 0 y 1000 (ambos incluidos). El valor predeterminado es de 90 días. Las garantías que caduquen según esta configuración se representan como  en el informe y el widget.
4. La casilla de verificación **Mostrar garantías caducadas**, que está marcada de forma predeterminada, se puede desactivar. Cuando se deja en blanco, OpenManage Enterprise deja de informar las garantías caducadas en todos los lugares donde se muestran las estadísticas relacionadas con la garantía.
5. Haga clic en **Aplicar** o **Descartar** para guardar la configuración de la garantía o para descartar los cambios y conservar la configuración anterior.

Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles

Para ir a la página Consola y extensiones, haga clic en **Configuración de la aplicación > Consola y extensiones**. En la página Consola y extensiones, puede hacer lo siguiente:

1. Ver la versión actual de su OpenManage Enterprise, comprobar si hay actualizaciones disponibles y, luego, actualizar a una versión más reciente. Puede hacer clic en el botón **Actualizar configuración** para realizar lo siguiente:
 - a. Comprobar si hay actualizaciones de forma automática o manual.
 - b. Elegir los modos En línea o Sin conexión para actualizar el dispositivo.Para obtener más información, consulte [Actualizar los ajustes en OpenManage Enterprise](#) en la página 151
2. Descargue e instale más extensiones (complementos), como la extensión Power Manager, para mejorar la funcionalidad del dispositivo. Para obtener más información acerca de la instalación de extensiones, consulte [Instalar una extensión](#) en la página 154

NOTA: Se requiere la licencia de OpenManage Enterprise Advanced para que las extensiones funcionen en su totalidad después de la instalación. Para obtener información más detallada sobre las extensiones, consulte la documentación correspondiente disponible en el sitio de soporte de Dell.

NOTA: Si instala una extensión en OpenManage Enterprise, reinicia los servicios del dispositivo.

3. Con las extensiones ya instaladas, puede hacer lo siguiente:

- Haga clic en el menú desplegable **Más acciones** para obtener más información acerca de la extensión o para deshabilitar, desinstalar, habilitar o cambiar la configuración de la extensión. Para obtener más información, consulte [Deshabilitar una extensión](#) en la página 155, [Desinstalación de una extensión](#) en la página 155, [Habilitación de una extensión](#) en la página 155
- Puede hacer clic en **Actualización disponible** siempre y cuando haya disponible nuevas versiones de las extensiones.

Información relacionada

[Actualización de Dell.com](#) en la página 152

[Actualización de un recurso compartido de red interna](#) en la página 153

Actualizar los ajustes en OpenManage Enterprise

Cuando hace clic en **Ajustes de configuración** en la página Consola y extensiones (**Ajustes de la aplicación** > **Consola y extensiones**), se pueden seleccionar los siguientes ajustes de actualización:

1. **Cómo buscar actualizaciones:** seleccione entre los siguientes métodos:
 - a. **Automático:** el dispositivo comprueba la disponibilidad de las actualizaciones automáticamente todos los lunes desde la fuente especificada en **Dónde buscar actualizaciones**.
 - b. **Manual:** cuando se configura en Manual, el usuario tiene que comprobar manualmente la disponibilidad de la actualización de la fuente especificada en **Dónde buscar actualizaciones**.
2. **Dónde buscar actualizaciones:** se puede especificar la ubicación desde donde el dispositivo busca actualizaciones. Las siguientes opciones se encuentran disponibles:
 - a. **Dell.com** (en línea): cuando se selecciona esta opción, el dispositivo comprueba la disponibilidad de la actualización directamente desde https://downloads.dell.com/openmanage_enterprise.
 - b. **Recurso compartido de red** (offline): especifique una ruta de acceso NFS, HTTP o HTTPS que contenga el paquete de actualización. Haga clic en **Probar ahora** para validar la conexión al recurso compartido de red especificado.
3. Seleccione la casilla de verificación **Iniciar automáticamente la actualización de la consola cuando se completen las descargas** para iniciar la instalación de la actualización de la consola inmediatamente después de descargar el paquete de actualización. Por lo demás, la actualización se puede iniciar manualmente.

NOTA: Según los ajustes de la actualización, el dispositivo comprueba la disponibilidad de una actualización y, si hay una nueva versión disponible, se muestra un anuncio con la información de la nueva versión de actualización. En el anuncio, el administrador puede optar por descartar la notificación, solicitar un recordatorio para más tarde o hacer clic en **Ver ahora** para conocer los detalles, como la versión y el tamaño de la actualización disponible en la página **Ajustes de la aplicación** > **Consola y extensiones**. En la sección OpenManage Enterprise de la página de la Consola y extensiones, se muestran todas las nuevas funciones y mejoras de la actualización disponible. Haga clic en **Actualizar para iniciar la actualización**.

Actualizar OpenManage Enterprise

Según los ajustes de la actualización (**Ajustes de la aplicación** > **Consola y extensiones** > **Ajustes de la actualización**), el OpenManage Enterprise existente se puede actualizar de forma automática o manual desde el sitio Dell.com directamente o desde un paquete de actualización ya descargado en el recurso compartido de red.

Cuando se identifica una versión nueva y actualizable de OpenManage Enterprise, se muestran detalles adicionales, como la versión, el tamaño y las nuevas funciones de la actualización, en la página Consola y extensiones, y hay un botón de **actualización** activo disponible. Además, se muestra un anuncio con detalles de la nueva versión. Todos los usuarios pueden ver el anuncio, sin embargo, solo los usuarios con privilegio de administrador pueden seleccionar la opción para recordar más tarde o descartar el mensaje.

NOTA: Solo las versiones 3.2 y posteriores de OpenManage Enterprise se pueden actualizar directamente a la versión 3.4 mediante el método Automático > En línea. Sin embargo, para actualizar desde OpenManage Enterprise Tech Release (versión 1.0), primero debe actualizar el dispositivo a las versiones 3.0 o 3.1 usando el método Manual > Sin conexión después de descargar el dispositivo a un recurso compartido local.

Antes de actualizar a la versión más reciente, el administrador debería:

- Tome una captura de la consola en la máquina virtual como copia de seguridad en caso de que ocurriera algo inesperado. Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario.
- Asigne por lo menos una hora para el proceso de actualización. Asigne tiempo adicional si se debe descargar la actualización mediante una conexión de red más lenta.
- Asegúrese de que no se ejecuten tareas de configuración, implementación o extensión (plugin) de dispositivos ni que se programen sus respectivas ejecuciones durante el tiempo de inactividad planificado. Todas las políticas o tareas activas o programadas se cierran sin advertencia durante la actualización.
- Notifique a los demás usuarios de la consola sobre la próxima actualización programada.
- Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente.

NOTA:

- Cuando actualice OpenManage Enterprise y cuente con más de 8000 dispositivos detectados, la tarea de actualización se completará dentro de dos o tres horas. Durante este período, es posible que los servicios no respondan. Se recomienda reiniciar el dispositivo de forma ordenada. Después de reiniciarlo, la funcionalidad normal del dispositivo se restaura.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de detección se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.
- En el caso de futuras actualizaciones de OpenManage Enterprise versión 3.4, si hace clic en Actualizar, se iniciará un trabajo de Descarga del paquete de actualización. Este trabajo se completa por su cuenta después de que se descarguen todos los archivos de actualización y el usuario no puede finalizarlo.

1. Para actualizar en línea desde Dell.com, consulte [Actualización de Dell.com](#) en la página 152.
2. Para realizar la actualización offline desde un paquete de actualización ya descargado en el recurso compartido de red NFS o HTTPS, consulte [Actualización de un recurso compartido de red interna](#) en la página 153.

NOTA: Según si se necesita una actualización mínima o completa, el administrador debe crear las estructuras de carpetas adecuadas antes de descargar el paquete de actualización. Para obtener más información acerca de las estructuras de carpetas permitidas y la actualización de OpenManage Enterprise a la versión más reciente, consulte la documentación técnica *Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise* en el sitio de soporte.

Actualización de Dell.com

El OpenManage Enterprise existente se puede actualizar en línea, ya sea de forma automática o manual, desde Dell.com (https://downloads.dell.com/openmanage_enterprise).

Requisitos previos para la actualización en línea:

- Los ajustes de la actualización **Dónde buscar actualizaciones** se debe especificar como Dell.com. Para obtener más información, consulte [Actualizar los ajustes en OpenManage Enterprise](#) en la página 151.
- Debe asegurarse de que el dispositivo OpenManage Enterprise pueda acceder a Dell.com y a la actualización prevista.
- Antes de comenzar la actualización, asegúrese de tomar una captura de la consola en la máquina virtual como respaldo en caso de que ocurra algo inesperado. Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario.

Cuando se identifica una versión nueva y actualizable de OpenManage Enterprise, se muestran detalles adicionales, como la versión, el tamaño y las nuevas funciones de la actualización, en la página Consola y extensiones, y hay un botón de **actualización** activo disponible. Además, se muestra un anuncio con detalles de la nueva versión. Todos los usuarios pueden ver el anuncio, sin embargo, solo los usuarios con privilegio de administrador pueden seleccionar la opción para recordar más tarde o descartar el mensaje.

1. Haga clic en **Actualizar** y realice una actualización.

NOTA:

- **Cuando hace clic en Actualizar, se inicia un trabajo de Descarga del paquete de actualización. Este trabajo se completa por sí mismo después de que se descarguen todos los archivos de actualización y no se puede finalizar.**
- **Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente**

2. Inicie sesión después de la actualización y confirme que el producto funcione según lo esperado. Compruebe el registro de auditoría de todas las advertencias o los errores relacionados con la actualización. Si se producen errores, exporte el registro de auditoría y guárdelo para solicitar asistencia técnica.

Una vez que se actualiza el dispositivo:

- Borre la caché del explorador. Si no borra la memoria caché del navegador, es posible que ocurran errores en las tareas nuevas después de la actualización.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de descubrimiento se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.

Tareas relacionadas

Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles en la página 150

Actualización de un recurso compartido de red interna

Debe configurar un recurso compartido de red local y descargar manualmente el paquete de actualización cuando no se conecta automáticamente a Dell.com. Se crea un registro de auditoría después de cada intento de buscar una actualización manualmente.

NOTA:

- **Cuando se actualizan recursos compartidos locales en una actualización manual de las versiones sin extensiones o complementos instalados (como 3.1 y 3.2), el registro de auditoría muestra entradas de advertencia, como "no se puede recuperar el archivo de origen del tipo catálogo de extensión porque el archivo no existe" y "el estado de descarga del catálogo de extensión contiene errores". Estos mensajes de error no tienen ningún impacto funcional en el proceso de actualización y se pueden omitir.**
- **Para obtener más información detallada sobre cómo actualizar OpenManage Enterprise a la versión más reciente, consulte la documentación técnica Actualizar la versión del dispositivo Dell EMC OpenManage Enterprise en el sitio de soporte (https://downloads.dell.com/manuals/all-products/esuprt_software/esuprt_ent_sys_mgmt/dell-openmanage-enterprise-v321_white-papers10_en-us.pdf).**
- **No se admite una actualización directa de la versión OpenManage Enterprise Tech Release. Las versiones Tech Release se deben actualizar primero a la versión 3.0 o 3.1 de OpenManage Enterprise.**
- **No se admite la actualización de OpenManage Enterprise versión 3.0 a la versión 3.4 mediante un recurso compartido de archivos de red (NFS). Sin embargo, puede actualizar el dispositivo desde la versión 3.1 o superior a través del NFS compartido.**

Antes de comenzar la actualización:

- asegúrese de tomar una instantánea de la consola en la máquina virtual como respaldo en caso de que ocurra algo inesperado. (Considere tiempo de inactividad adicional para esta tarea, en caso de ser necesario).
- Si la actualización falla, el dispositivo se reiniciará. Se recomienda revertir la instantánea de la VM y actualizarla nuevamente.
- La adición de una segunda interfaz de red solo se debe realizar después de que se completen las tareas de actualización posteriores a la consola. Intentar agregar una segunda NIC mientras la tarea posterior a la actualización está en progreso producirá resultados infructuosos.

- Debe asegurarse de que los certificados de seguridad estén firmados por una autoridad de certificación de terceros de confianza cuando utilice el método de actualización HTTPS.

Para actualizar OpenManage Enterprise, realice las siguientes acciones:

1. Descargue los archivos correspondientes en <https://downloads.dell.com>, guárdelos en un recurso compartido de red y conserve la misma estructura de carpetas a la que se puede acceder a través de la consola.
2. Seleccione **Manual** y **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: `nfs://<Dirección IP>/<Nombre_carpeta>`, `http://<Dirección IP>/<Nombre_carpeta>`, `https://<Dirección IP>/<Nombre_carpeta>`.
Se muestra la versión de actualización disponible con una breve descripción de las nuevas funciones.
4. Para validar la conexión al catálogo, haga clic en **Probar ahora**. Si se establece la conexión con el catálogo, aparecerá el mensaje *Conexión correcta*. Si no se establece la conexión con la dirección del recurso compartido o la ruta del archivo del catálogo, aparecerá el mensaje *Error de conexión a la ruta*. Este paso es opcional.
5. Haga clic en **Actualizar** y realice una actualización (aplicable para futuras actualizaciones).

NOTA:

- **Cuando hace clic en Actualizar, se inicia un trabajo de Descarga del paquete de actualización. Este trabajo finaliza por su cuenta después de que se descargan todos los archivos de actualización y el usuario no puede finalizarlo**
- **Si durante la descarga de la actualización ocurre un problema de conexión a través de proxy, desmarque la configuración de proxy y, luego, realice la descarga.**

Inicie sesión después de la actualización y confirme que el producto funcione según lo esperado. Compruebe el registro de auditoría de todas las advertencias o los errores relacionados con la actualización. Si se producen errores, exporte el registro de auditoría y guárdelo para solicitar asistencia técnica.

Una vez que se actualiza el dispositivo:

- Borre la caché del explorador. Si no borra la memoria caché del navegador, es posible que ocurran errores en las tareas nuevas después de la actualización.
- Si realiza la actualización desde OpenManage Enterprise versión 3.1, se recomienda volver a configurar o importar los grupos de Active Directory para mejorar el rendimiento.
- Puede iniciar sesión inmediatamente después de que el dispositivo se actualice y no es necesario esperar hasta que se descubra todo el inventario. Después de la actualización, la tarea de descubrimiento se ejecutará en segundo plano y podrá ver el progreso de forma ocasional.

Tareas relacionadas

[Comprobar y actualizar la versión de OpenManage Enterprise y las extensiones disponibles](#) en la página 150

Instalar una extensión

Instale una extensión según sus requisitos para mejorar la funcionalidad de OpenManage Enterprise.

- Asegúrese de que la conectividad con el repositorio sea correcta.
 - Para el modo En línea, es el portal `download.Dell.com`.
 - Para el modo Sin conexión, el servidor de está configurado con los archivos de instalación de extensión y el catálogo de extensión requeridos.

NOTA: Si instala una extensión en OpenManage Enterprise, reinicia los servicios del dispositivo.

Para instalar una extensión, siga estos pasos:

1. Haga clic en **Configuración de la aplicación > Consola y extensiones**.
Se muestra la página Consola y extensiones
2. En la sección Extensiones, al lado de la extensión que desea instalar, haga clic en **Más acciones > Instalar**.
Se muestra la ventana Instalar extensión.
3. Revise la sección Prerrequisitos y asegúrese de que cumple con la lista de requisitos previos que se menciona ahí.
NOTA: Las listas de requisitos previos cambian a medida que selecciona la versión de extensión que desea instalar.
4. En **Detalles de instalación**, seleccione la versión requerida de la extensión en el menú desplegable Versiones y, luego, haga clic en Instalar extensión.

En la ventana Confirmación, aparecen detalles acerca de la cantidad de usuarios que inició sesión en OpenManage Enterprise, las tareas en curso y los trabajos programados.

Para confirmar la instalación, seleccione **Acepto que he capturado la instantánea del dispositivo OM Enterprise antes de la opción Actualizar** y, luego, haga clic en **Confirmar instalación**.

Aparece el estado de la instalación.

Deshabilitar una extensión

Desactiva toda la funcionalidad de la extensión en OpenManage Enterprise.

NOTA: La deshabilitación de una extensión en OpenManage Enterprise reinicia los servicios del dispositivo.

1. Haga clic en **Configuración de la aplicación > Consola y extensión**
Se muestra la página Consola y extensiones.
2. En la sección Extensiones, haga clic en **Más acciones > Deshabilitar**
Se muestra la ventana Deshabilitar extensión
3. Haga clic en **Deshabilitar extensión**, luego, en la ventana de confirmación, seleccione **Acepto que he capturado la instantánea del dispositivo OM Enterprise antes de la opción Actualizar** y haga clic en **Deshabilitar extensión**.

NOTA: Después de deshabilitar la extensión, no podrá ver ninguna información o página relacionada con la extensión en OpenManage Enterprise.

Desinstalación de una extensión

Desinstala y elimina todos los datos que recolecta la extensión.

1. Haga clic en **Configuración de la aplicación > Consola y extensiones**.
Se muestra la página Consola y extensiones.
2. En la sección **Extensiones**, haga clic en **Más configuraciones > Desinstalar**
Se muestra la ventana Desinstalar extensión.
3. Haga clic en **Desinstalar extensión**, luego, en la ventana de confirmación, seleccione **Acepto que he capturado la instantánea del dispositivo OM Enterprise antes de la opción Actualizar** y haga clic en **Desinstalar extensión**.

Habilitación de una extensión

Se muestran todas las páginas de la extensión en OpenManage Enterprise y se habilita la funcionalidad de la extensión en OpenManage Enterprise.

NOTA: La habilitación de una extensión en OpenManage Enterprise reinicia los servicios del dispositivo.

1. Haga clic en **Configuración de la aplicación > Consola y extensiones**.
Se muestra la página Consola y extensiones.
2. En la sección Extensiones, haga clic en **Más acciones > Habilitar**
Se muestra la ventana Habilitar.
3. Haga clic en **Habilitar extensión** y, en la ventana Confirmación, seleccione la opción **I agree that I have captured the snapshot of the OM Enterprise appliance prior to the upgrade** y haga clic en **Habilitar extensión**.

Ejecutar comandos y scripts remotos

Cuando recibe una SNMP trap, puede ejecutar un script en OpenManage Enterprise. Esto establece una política que abre un vale en el sistema de generación de vales de terceros para la administración de alertas. Puede crear y almacenar solo hasta **cuatro** comandos remotos.

1. Haga clic en **Configuración de la aplicación > Ejecución del script**.
2. En la sección **Configuración de comandos remotos**, haga lo siguiente:
 - a. Para agregar un comando remoto, haga clic en **Crear**.
 - b. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - c. Seleccione uno de los siguientes tipos de comando:
 - i. Script

- ii. RACADM
 - iii. Herramienta IPMI
- d. Si selecciona **Script**, haga lo siguiente:
- i. En la casilla **Dirección IP**, ingrese la dirección IP.
 - ii. Seleccione el método de autenticación: **contraseña** o **clave SSH**.
 - iii. Especifique el **Nombre de usuario** y la **Contraseña** o la **clave SSH**.
 - iv. En la casilla **Comando**, escriba los comandos.
 - Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - La sustitución de token en secuencias de comandos es posible. Consulte [Sustitución del token en secuencias de comandos remotas y política de alerta](#) en la página 163
 - v. Haga clic en **Finalizar**.
- e. Si selecciona **RACADM**, haga lo siguiente:
- i. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - iii. Haga clic en **Finalizar**.
- f. Si selecciona **Herramienta IPMI**, haga lo siguiente:
- i. En la casilla **Nombre del comando**, escriba el nombre del comando.
 - ii. En la casilla **Comando**, escriba los comandos. Se pueden ingresar un máximo de 100 comandos, los cuales deben estar en líneas separadas.
 - iii. Haga clic en **Finalizar**.
3. Para editar la configuración de los comandos remotos, seleccione el comando y haga clic en **Editar**.
4. Para eliminar la configuración de los comandos remotos, seleccione el comando y haga clic en **Eliminar**.

Configuración de OpenManage Mobile

OpenManage Mobile (OMM) es una aplicación de administración de sistemas que permite realizar de forma segura un subconjunto de tareas de reparación y supervisión de los centros de datos en una o varias consolas de OpenManage Enterprise o integrated Dell Remote Access Controllers (iDRAC) mediante un dispositivo Android o iOS. Mediante OMM puede:

- Recibir notificaciones de alertas desde OpenManage Enterprise.
- Ver información del grupo, el dispositivo, alertas y registros.
- Encender, apagar o reiniciar un servidor.

De manera predeterminada, las notificaciones de inserción están activadas para todas las alertas y las alertas críticas. Este capítulo proporciona información sobre los ajustes de OMM que puede configurar a través de OpenManage Enterprise. También proporciona información necesaria para solucionar los problemas de OMM.

 **NOTA:** Para obtener información sobre la instalación y el uso de OMM, consulte la *Guía del usuario de OpenManage Mobile* en Dell.com/OpenManageManuals.

Tareas relacionadas

- [Activación o desactivación de notificaciones de alerta de OpenManage Mobile](#) en la página 157
- [Activación o desactivación de suscriptores de OpenManage Mobile](#) en la página 157
- [Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158
- [Visualización del estado del servicio de notificación de alertas](#) en la página 158
- [Solución de problemas de OpenManage Mobile](#) en la página 160

Información relacionada

- [Activación o desactivación de notificaciones de alerta de OpenManage Mobile](#) en la página 157
- [Activación o desactivación de suscriptores de OpenManage Mobile](#) en la página 157
- [Solución de problemas de OpenManage Mobile](#) en la página 160

Activación o desactivación de notificaciones de alerta de OpenManage Mobile

De manera predeterminada, OpenManage Enterprise está configurado para enviar notificaciones de alerta a la aplicación OpenManage Mobile. Sin embargo, las notificaciones de alerta se envían desde OpenManage Enterprise solo cuando un usuario de OpenManage Mobile agrega OpenManage Enterprise a la aplicación de OpenManage Mobile.

NOTA: Se requieren privilegios de administrador para activar o desactivar las notificaciones de alerta en OpenManage Mobile.

NOTA: Para que OpenManage Enterprise envíe notificaciones de alerta a OpenManage Mobile, asegúrese de que el servidor de OpenManage Enterprise tenga acceso a Internet (HTTPS) de salida.

Para activar o desactivar las notificaciones de alerta de OpenManage Enterprise a OpenManage Mobile, realice lo siguiente:

1. Haga clic en **OpenManage Enterprise > Configuración de la aplicación > Móvil**.
2. Marque la casilla **Activar envío de notificaciones push**.
3. Haga clic en **Aplicar**.

Tareas relacionadas

[Configuración de OpenManage Mobile](#) en la página 156

Información relacionada

[Configuración de OpenManage Mobile](#) en la página 156

[Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158

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](#) en la página 156


Información relacionada

[Configuración de OpenManage Mobile](#) en la página 156

[Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158

Eliminación de un suscriptor de OpenManage Mobile

Si se elimina un suscriptor de OpenManage Mobile, se elimina al usuario de la lista de suscriptores, lo que impide que este reciba las notificaciones de alerta de OpenManage Enterprise. Sin embargo, el usuario de OpenManage Mobile puede volver a suscribirse más tarde a las notificaciones de alerta desde la aplicación OpenManage.

 **NOTA:** Se requieren derechos de administrador para eliminar a un suscriptor de OpenManage Mobile.

Para eliminar un suscriptor de OpenManage Mobile:

1. Haga clic en **OpenManage Enterprise > Configuración de la aplicación > Móvil**.
2. Seleccione la casilla de verificación correspondiente al suscriptor y haga clic en **Eliminar**.
3. Cuando se lo solicite, haga clic en **Sí**.

Tareas relacionadas

[Activación o desactivación de notificaciones de alerta de OpenManage Mobile](#) en la página 157

[Activación o desactivación de suscriptores de OpenManage Mobile](#) en la página 157

[Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158

[Visualización del estado del servicio de notificación de alertas](#) en la página 158

Información relacionada

[Configuración de OpenManage Mobile](#) en la página 156

[Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158

Visualización del estado del servicio de notificación de alertas

OpenManage Enterprise reenvía las notificaciones de alerta a los suscriptores de OpenManage Mobile a través de su respectivo servicio de notificación de alertas de la plataforma del dispositivo. Si el suscriptor de OpenManage Mobile no pudo recibir notificaciones de alerta, puede comprobar el **Estado del servicio de notificación** para solucionar problemas con la entrega de las notificaciones de alerta.

Para ver el estado del servicio de notificación de alertas, haga clic en **Configuración de la aplicación > Móvil**.

Tareas relacionadas

[Visualización del estado del servicio de notificación de alertas](#) en la página 158

Información relacionada

[Configuración de OpenManage Mobile](#) en la página 156

[Eliminación de un suscriptor de OpenManage Mobile](#) en la página 158

[Visualización del estado del servicio de notificación de alertas](#) en la página 158

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 28. 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.

Tabla 28. Estado del servicio de notificación (continuación)

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 29. 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 30. 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: <ul style="list-style-type: none"> • 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 <i>Guía del usuario de OpenManage Mobile</i> y vuelva a conectar el dispositivo a OpenManage Enterprise. Si el dispositivo ya no está conectado a OpenManage Enterprise, quite al suscriptor.
El servicio de reenvío de mensajes rechaza el registro de OpenManage Enterprise. [Código 154]	Se está usando una versión obsoleta de OpenManage Enterprise.	Actualice a una versión más reciente de OpenManage Enterprise.

Tareas relacionadas

[Configuración de OpenManage Mobile](#) en la página 156

Información relacionada

[Configuración de OpenManage Mobile](#) en la página 156

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](#)
- [Definiciones de los campos de la línea base de firmware](#)
- [Definiciones de los campos Programar trabajos](#)
- [Categorías de alerta después de la reubicación de EEMI](#)
- [Sustitución del token en secuencias de comandos remotas y política de alerta](#)
- [Flujo de depuración de servicio de campo](#)
- [Desbloquear la capacidad FSD](#)
- [Instalar o conceder un archivo DAT.ini firmado de FSD](#)
- [Llamar FSD](#)
- [Desactivar FSD](#)
- [Definiciones de campos de administración de catálogos](#)
- [Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge](#)

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, consulte [Crear una base](#) en la página 59.
- **CATÁLOGO:** el catálogo de firmware al cual pertenece la línea base de firmware. Consulte [Administrar catálogos de firmware y controladores](#) en la página 56.
- **HORA DE ÚLTIMA EJECUCIÓN:** la hora en la cual el informe de cumplimiento de línea base se ejecutó por última vez. Consulte [Comprobar el cumplimiento del firmware y los controladores de un dispositivo](#) en la página 60.

Definiciones de los campos Programar trabajos

- **Ejecutar ahora** para iniciar el trabajo inmediatamente.

- **Ejecutar más tarde** para especificar una fecha y hora posteriores.
- **Ejecutar según el programa** para ejecutar repetidamente según la frecuencia seleccionada. Seleccione **Diariamente** y, a continuación, seleccione correctamente la frecuencia.

NOTA: De manera predeterminada, el reloj del programador de trabajos se restablece a las 00:00 todos los días. El formato de cron no considera la hora de creación del trabajo cuando se calcula la frecuencia del trabajo. Por ejemplo, si un trabajo se inicia a las 10:00, y se debe ejecutar cada 10 horas, la próxima vez que se ejecute el trabajo será a las 20:00. Sin embargo, la siguiente vez no será a las 06:00 del día siguiente, sino a las 00:00, ya que el reloj del programador se restablece a las 00:00 todos los días.

Categorías de alerta después de la reubicación de EEMI

Tabla de reubicaciones de EEMI

Tabla 31. Categorías de alerta en OpenManage Enterprise

Categoría anterior	Subcategoría anterior	Nueva categoría	Nueva subcategoría
Auditorías	Dispositivos	Condición del sistema	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Dispositivos	Configuración	Dispositivos
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Aplicación	Configuración	Aplicación
Auditorías	Dispositivos	Auditorías	Usuarios
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Auditorías	Plantillas	Configuración	Plantillas
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Trabajo
Configuración	Inventario	Configuración	Dispositivos
Configuración	Inventario	Configuración	Dispositivos
Configuración	Inventario	Configuración	Dispositivos
Configuración	Firmware	Configuración	Trabajos
Configuración	Firmware	Configuración	Trabajos
Varios	Trabajos	Configuración	Trabajos

Tabla 31. Categorías de alerta en OpenManage Enterprise (continuación)

Categoría anterior	Subcategoría anterior	Nueva categoría	Nueva subcategoría
Varios	Trabajos	Configuración	Trabajos
Varios	Trabajos	Configuración	Trabajos
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Generic	Configuración	Generic
Varios	Dispositivos	Configuración	Dispositivos
Varios	Dispositivos	Configuración	Dispositivos
Auditorías	Seguridad	Configuración	Seguridad
Auditorías	Seguridad	Configuración	Seguridad
Auditorías	Seguridad	Configuración	Seguridad

Sustitución del token en secuencias de comandos remotas y política de alerta

OpenManage Enterprise admite el uso de tokens para mejorar secuencias de comandos remotas y la creación de políticas de alertas.

Tabla 32. Tokens admitidos en OpenManage Enterprise

Tokens	Descripción
\$IP	Dirección IP del dispositivo
\$MSG	Mensaje
\$DATE	Fecha
\$TIME	Hora
\$SEVERITY	Gravedad
\$SERVICETAG	Etiqueta de servicio
\$RESOLUTION	Resolución recomendada
\$CATEGORY	Nombre de categorías de alertas
\$ASSETTAG	Etiqueta de propiedad
\$MODEL	Nombre del modelo

Flujo de depuración de servicio de campo

En OpenManage Enterprise, puede autorizar la depuración de la consola mediante la opción depuración el servicio de campo (FSD).

Mediante el uso de FSD, puede realizar las siguientes tareas:

- Permitir la activación y la copia de los registros de depuración

- Permitir la copia de los registros en tiempo real
- Permitir la creación de una copia de seguridad o la restauración de archivos de base de datos a VM.

Los temas a los que se hace referencia en cada tarea proporcionan instrucciones detalladas. Para activar FSD, realice las siguientes tareas:

1. Desbloquear la capacidad de FSD. Consulte [Desbloquear la capacidad FSD](#) en la página 164.
2. Instalar o conceder archivo DAT.ini firmado de FSD. Consulte [Instalar o conceder un archivo DAT.ini firmado de FSD](#) en la página 164.
3. Llamar FSD. Consulte [Llamar FSD](#) en la página 165.
4. Desactivar FSD. Consulte [Desactivar FSD](#) en la página 165.

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.

Convención de nomenclatura genérica para servidores de Dell EMC PowerEdge

Para cubrir una variedad de modelos de servidores, ahora se hace referencia a los servidores PowerEdge mediante la convención de nomenclatura genérica y no mediante su generación.

En este tema se explica cómo identificar la generación de un servidor PowerEdge al que se hace referencia utilizando la convención de nomenclatura genérica.

Por ejemplo:

El modelo del servidor R740 es un sistema de rack que cuenta con dos procesadores de la 14.^a generación de servidores con procesadores Intel. En la documentación de, para referirse a R740, se utiliza el servidor **YX4X** con la convención de nomenclatura genérica y estas siglas hacen referencia a lo siguiente:

- La letra **Y** (alfabeto) indica el tipo (factor de forma: nube [C], flexible [F], modular [M o MX], rack [R], torre [T]) del servidor.
- La letra **X** (dígito) señala la clase (número de procesadores) del servidor.
- El dígito **4** indica la generación del servidor.
- La letra **X** (dígito) señala la marca del procesador.

Tabla 33. Convención de nomenclatura de servidores PowerEdge junto con ejemplos

Servidores YX3X	Sistemas YX4X
PowerEdge M630	PowerEdge M640
PowerEdge M830	PowerEdge R440
PowerEdge T130	PowerEdge R540