Dell EMC OpenManage Server Administrator versión 9.1

Guía del usuario

Noviembre 2020
Rev. A01

DELL Technologies

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

1

Introducción

Server Administrator proporciona una solución de administración de sistemas individual y completa de dos maneras: desde una interfaz de usuario gráfica (GUI) integrada basada en la web y desde una interfaz de línea de comandos (CLI) a través del sistema operativo. Server Administrator permite a los administradores de sistemas administrar sistemas de forma local y remota en una red. Permite a los administradores de sistemas centrarse en la administración de toda su red mediante la administración de sistemas individual e integral. En el contexto de Server Administrator, un sistema hace referencia a un sistema independiente, un sistema con unidades de almacenamiento de red conectadas en un chasis separado o un sistema modular que consta de uno o varios módulos de servidor en un gabinete modular. Server Administrator proporciona información sobre:

- Sistemas que funcionan correctamente y sistemas que presentan problemas
- Sistemas que requieren operaciones de recuperación remota

Server Administrator proporciona administración fácil de usar de sistemas locales y remotos a través de un conjunto completo de servicios de administración integrada. Server Administrator es la única instalación en el sistema que se está administrando y a la que se puede acceder de forma local y remota desde la página de inicio de **Server Administrator**. Es posible acceder a los sistemas supervisados de forma remota a través de conexiones dial-in, LAN o inalámbricas. Server Administrator garantiza la seguridad de sus conexiones de administración a través del control de acceso basado en funciones (RBAC), de la autenticación y del cifrado de capa de sockets seguros (SSL).

Temas:

Instalación

Puede instalar Server Administrator mediante el software *Herramientas y documentación de Dell EMC Systems Management*. Este software proporciona un programa de instalación para instalar, actualizar y desinstalar componentes de software de Server Administrator, el sistema administrado y la estación de administración. Además, puede instalar Server Administrator en varios sistemas mediante una instalación desatendida a través de una red. El instalador de Server Administrator proporciona scripts de instalación y paquetes RPM para instalar y desinstalar Server Administrator y otros componentes de software para el sistema administrado. Para obtener más información, consulte la *Guía de instalación de Dell EMC Server Administrator* y la *Guía de instalación del software Management Station* en **dell.com/opemanagemanuals**.

NOTA: Cuando instala los paquetes de código abierto desde el software *Herramientas y documentación de Dell EMC Systems Management*, los archivos de licencia correspondientes se copian automáticamente en el sistema. Al eliminar estos paquetes, los archivos de licencia correspondientes también se eliminan.

NOTA: Si tiene un sistema modular, instale Server Administrator en cada uno de los módulos de servidor instalado en el chasis.

Novedades de esta versión

Los elementos más destacados de la versión OpenManage Server Administrator son:

- Compatibilidad con Java Runtime Environment 8, actualización 131
- Versión de Tomcat actualizada a la 8.5.15
- La versión mínima admitida de TLS es TLSv1.1
- La lista Encryption Ciphers se actualizó según los estándares de seguridad OWASP Apache Tomcat
- Admite la supervisión NVDIMM (módulo DIMM no volátil) en los servidores PowerEdge de 14G
- Admite el modo de bloqueo de la configuración del sistema en los servidores PowerEdge de 14G
- Admite la función "Ciclo completo de alimentación" en la configuración de la BIOS, que permite activar el ciclo de corriente continua seguido por un ciclo de corriente alterna de los componentes auxiliares (incluye iDRAC, CPLD, etc.)

- Desde la 14.ª generación en adelante, el servicio compartido Server Administrator, que se utiliza para activar el recopilador de inventario, se desactivará de manera predeterminada durante la instalación de Server Administrator. Con el fin de activar el recopilador de inventario de manera explícita, el cliente debe activarlo mediante la interfaz de línea de comandos de OM

- Compatibilidad con los siguientes sistemas operativos:
  - Red Hat Enterprise Linux 7.4
  - Red Hat Enterprise Linux 6.9
  - SUSE Linux Enterprise Server 12 SP3
  - SUSE Linux Enterprise Server 11 SP4
  - VMware ESXi 6.5
  - VMware ESXi 6.0 U3
  - Ubuntu 16.04.3 LTS (Xenial Xerus) desde servidores PowerEdge de 14G en adelante
  - **NOTA:** Server Administrator y Storage Management ya no son compatibles con el sistema operativo Citrix XenServer.
- Compatibilidad con los siguientes exploradores:
  - Internet Explorer: 10, 11
  - Google Chrome: 57, 58
  - Safari - 10.x
  - Mozilla Firefox - 52, 53
- Las tarjetas de red admitidas son:
  - Adaptador de altura completa Fibre Channel Emulex LightPulse LPe31000-M6-D 1 puerto de 16 Gb
  - Adaptador de bajo perfil Fibre Channel Emulex LightPulse LPe31000-M6-D 1 puerto de 16 Gb
  - Adaptador de altura completa Fibre Channel Emulex LightPulse LPe31002-M6-D 2 puertos de 16 Gb
  - Adaptador de bajo perfil Fibre Channel Emulex LightPulse LPe31002-M6-D 2 puertos de 16 Gb
  - Adaptador de bajo perfil Mellanox ConnectX-4 de dos puertos EDR VPI QSFP28
  - Adaptador de altura completa Mellanox ConnectX-4 de dos puertos EDR VPI QSFP28
  - Adaptador de bajo perfil Mellanox ConnectX-4 de puerto único EDR VPI QSFP28
  - Adaptador de altura completa Mellanox ConnectX-4 de puerto único EDR VPI QSFP28
  - Canal de puerto: adaptador Intel(R) Ethernet 25G 2P XXV710 (adaptador PCIe 25GBE)
  - QLogic Duluth (FH): adaptador de red convergente con formato punta de flecha BT de dos puertos de 10 GB QL41162HFRJ-DL-BK (sin componentes ópticos)
  - QLogic Duluth (LP): adaptador de red convergente con formato punta de flecha BT de dos puertos de 10 GB QL41162HLRJ-DL-BK (sin componentes ópticos)
  - QLogic Dunkirk (10-FH): adaptador de red convergente con formato punta de flecha SFP de dos puertos de 10 GB QL41112HFCU-DL-BK (sin componentes ópticos)
  - QLogic Dunkirk (10-LP): adaptador de red convergente con formato punta de flecha SFP de dos puertos de 10 GB QL41112HLCU-DL-BK (sin componentes ópticos)
  - QLogic Dunkirk (FH): adaptador de red convergente con formato punta de flecha SFP28 de dos puertos de 10/25 GB QL41262HFCU-DL-BK (sin componentes ópticos)
  - QLogic Dunkirk (LP): adaptador de red convergente con formato punta de flecha SFP28 de dos puertos de 10/25 GB QL41262HLCU-DL-BK (sin componentes ópticos)
  - QLogic Dundee (FH): adaptador de red convergente con formato punta de flecha BT de cuatro puertos de 10 GB QL41164HFRJ-DL (sin componentes ópticos)
  - QLogic Dundee (LP): adaptador de red convergente con formato punta de flecha BT de cuatro puertos de 10 GB QL41164HLRJ-DL (sin componentes ópticos)
  - QLogic Delray (FH): adaptador de red convergente con formato punta de flecha SFP de cuatro puertos de 10 GB QL41164HFCU-DL (sin componentes ópticos)
  - QLogic Delray (LP): adaptador de red convergente con formato punta de flecha SFP de cuatro puertos de 10 GB QL41164HLCU-DL (sin componentes ópticos)
  - QLogic Dardanelle (rNDC): adaptador de red convergente con formato punta de flecha SFP28 de dos puertos de 10/25 GB QL41262HMCU-DL (sin componentes ópticos)

- QLogic Darwin (rNDC): adaptador de red convergente con formato punta de flecha BT de dos puertos de 10 GB QL41164HMRJ-DL (sin componentes ópticos)
- QLogic Dresden (rNDC): adaptador de red convergente con formato punta de flecha SFP de dos puertos de 10 GB QL41164HMCU-DL (sin componentes ópticos)
- QLogic Dartmouth (rNDC): adaptador de red convergente con formato punta de flecha BT de puerto 2+2 de 10 GB y 1 GB QL41264HMCU-DL-BK (sin componentes ópticos)
- QLogic Dunedin (rNDC): adaptador de red convergente con formato punta de flecha SFP de puerto 2+2 de 10 GB y 1 GB QL41264HMCURJ-DL-BK (sin componentes ópticos)

NOTA: Para obtener la lista de sistemas operativos admitidos y servidores Dell, consulte la *Dell EMC OpenManage Software Support Matrix* (Matriz de compatibilidad de software de Dell EMC OpenManage) en la versión requerida del software **OpenManage** en **dell.com/openmanagemanuals**.

Actualización de los componentes individuales del sistema

Para actualizar componentes individuales del sistema, utilice los Dell Update Packages específicos de dichos componentes. Use el DVD *Dell Server Update Utility* para consultar el informe de versión completo y actualizar todo un sistema. La Server Update Utility (SUU) identifica y aplica las actualizaciones requeridas para el sistema. La SUU también puede descargarse desde **support.dell.com.**

NOTA: Para obtener más información sobre cómo obtener y usar la Server Update Utility (SUU), para actualizar el sistema o para ver las actualizaciones disponibles de cualquier sistema que se muestre en el repositorio, consulte la *Guía del usuario de Dell Server Update Utility* en **dell.com/openmanagemanuals**.

Storage Management Service

Storage Management Service proporciona información de administración de almacenamiento en una vista gráfica integrada.

NOTA: Para obtener más información sobre Storage Management Service, consulte la *Guía del usuario de Dell EMC Server Administrator Storage Management* en **dell.com/openmanagemanuals**.

Instrumentation Service

Instrumentation Service proporciona acceso rápido a información detallada sobre errores y rendimiento recopilada por agentes de administración de sistemas estándares de la industria , y permite la administración remota de sistemas supervisados, incluidos el apagado, el inicio y la seguridad.

Remote Access Controller

Remote Access Controller ofrece una solución integral de administración remota para los sistemas que cuentan con la solución de controlador de administración de la placa base (BMC)/Integrated Dell Remote Access Controller (iDRAC). Remote Access Controller proporciona acceso remoto a un sistema que no funciona, lo que le permite poner el sistema en funcionamiento lo más rápido posible. Remote Access Controller también envía una notificación de alerta cuando un sistema se encuentra inactivo y le permite reiniciar el sistema de forma remota. Además, Remote Access Controller registra la posible causa de los fallos del sistema y guarda la pantalla de bloqueo más reciente.

Registros

Server Administrator muestra registros de comandos emitidos al sistema o por este, eventos de hardware supervisados y alertas del sistema. Puede ver los registros en la página de inicio, imprimirlos o guardarlos como informes, y enviarlos por correo electrónico a un contacto de servicio designado.

Disponibilidad de estándares de administración de sistemas

Server Administrator admite los siguientes protocolos de administración de sistemas:

- Protocolo seguro de transferencia de hipertexto (HTTPS)
- Modelo común de información (CIM)
- Protocolo simple de administración de red (SNMP)

Si su sistema admite SNMP, instale y habilite el servicio en el sistema operativo. Si los servicios SNMP están disponibles en el sistema operativo, el programa de instalación de Server Administrator instala los agentes compatibles con SNMP.

Todos los sistemas operativos admiten HTTPS. La compatibilidad de CIM y SNMP depende del sistema operativo y, en ocasiones, de la versión del sistema operativo.

NOTA: Para obtener información sobre cuestiones de seguridad de SNMP, consulte el archivo de las notas de la versión de Server Administrator (incluido en la aplicación de Server Administrator) o en **dell.com/openmanagemanuals**. Aplique las actualizaciones desde los agentes maestros del SNMP del sistema operativo para garantizar que los subagentes del SNMP están seguros.

Disponibilidad en sistemas operativos compatibles

En los sistemas operativos Microsoft Windows compatibles, Server Administrator admite dos estándares de administración de sistemas: CIM/Instrumental de administración de Windows (WMI) y SNMP, mientras que en los sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server compatibles, Server Administrator admite el estándar de administración de sistemas de SNMP.

Server Administrator agrega seguridad considerable a estos estándares de administración de sistemas. Todas las operaciones Set de atributos (por ejemplo, cambiar el valor de una etiqueta de propiedad) deben realizarse con Dell EMC OpenManage Essentials mientras mantiene una sesión iniciada con los privilegios necesarios.

En la siguiente tabla se muestra la disponibilidad de los estándares de administración de sistemas para cada sistema operativo compatible.

Tabla 1. Disponibilidad de estándares de administración de sistemas

Sistema operativo	SNMP	CIM
Familia Windows Server 2012 R2	Disponible desde el medio de instalación del sistema operativo	Siempre instalado
Red Hat Enterprise Linux	Disponible en el paquete net-snmp desde el medio de instalación del sistema operativo	No disponible
SUSE Linux Enterprise Server	Disponible en el paquete net-snmp desde el medio de instalación del sistema operativo	No disponible
VMware ESXi	Compatibilidad con capturas SNMP disponible **NOTA:** Si bien ESXi admite capturas SNMP, no es compatible con el inventario de hardware a través de SNMP.	Disponible

Página principal de Server Administrator

La página principal de **Server Administrator** ofrece tareas de administración de sistemas basadas en explorador web fáciles de configurar y usar desde el propio sistema administrado o desde un host remoto a través de una LAN, un servicio de acceso telefónico o una red inalámbrica. Si el servicio de conexión del Server Administrator de Systems Management (servicio de conexión del DSM SA) está instalado y configurado en el sistema administrado, puede efectuar funciones de administración remota desde cualquier sistema que cuente con un explorador web y una conexión admitidos. Además, la página principal de Server Administrator proporciona una ayuda en pantalla completa y contextual.

Otros documentos que podrían ser de utilidad

Además de esta guía, puede acceder a las siguientes guías disponibles en **dell.com/softwaresecuritymanuals**.

- La *Matriz de compatibilidad de software de los sistemas Dell EMC* ofrece información sobre los diversos sistemas, los sistemas operativos admitidos por estos sistemas y los componentes que se pueden instalar en estos sistemas.
- La *Guía de instalación de Dell EMC OpenManage Server Administrator* contiene instrucciones de ayuda para instalar Dell EMC OpenManage Server Administrator.
- La *Guía de instalación del software para estaciones de administración Dell EMC OpenManage* contiene instrucciones de ayuda para instalar el software para estaciones de administración Dell EMC OpenManage.
- La *Guía de referencia del SNMP de Dell EMC OpenManage* describe la base de datos de información de administración (MIB) del protocolo simple de administración de redes (SNMP).
- La *Guía de referencia del CIM de Dell EMC OpenManage Server Administrator* describe el proveedor del modelo de información común (CIM), una extensión del archivo de formato de objeto de administración (MOF) estándar.
- En la *Guía de referencia de mensajes de Dell EMC* se presenta una lista de los mensajes que aparecen en el registro de alertas de la página principal de Server Administrator o en el visor de eventos del sistema operativo.
- La *Guía de la interfaz de la línea de comandos de Dell EMC OpenManage Server Administrator* describe la interfaz de la línea de comandos completa de Server Administrator.
- La *Guía del usuario de Dell Remote Access Controller* proporciona información completa sobre el uso de la utilidad de línea de comandos RACADM para configurar un DRAC.
- La *Guía del usuario de Dell Chassis Management Controller* proporciona información completa sobre el uso de la controladora que administra todos los módulos del chasis que contiene el sistema.
- La *Guía de referencia de la línea de comandos para el iDRAC6 y el CMC* proporciona información acerca de los subcomandos RACADM, las interfaces admitidas, los grupos de bases de datos de propiedad y las definiciones de objeto para el iDRAC6 y el CMC.
- La *Guía del usuario de Integrated Dell Remote Access Controller 7 (iDRAC7)* proporciona información sobre cómo configurar y usar iDRAC7 para servidores blade, de torre y bastidor de 12º generación a fin de administrar y supervisar el sistema y sus recursos compartidos en forma remota a través de una red.
- La *Guía del usuario de Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade* proporciona información sobre cómo configurar y usar un iDRAC6 para servidores blade de 11º generación a fin de administrar y supervisar el sistema y sus recursos compartidos en forma remota a través de una red.
- La *Guía del usuario de Integrated Dell Remote Access Controller 6 (iDRAC6)* proporcina información completa sobre cómo configurar y usar un iDRAC6 para servidores de torre y bastidor de 11.ª generación a fin de administrar y supervisar el sistema y sus recursos compartidos de forma remota a través de una red.
- *Guía del usuario de Dell Online Diagnostics* contiene información completa sobre cómo instalar y usar Online Diagnostics en el sistema.
- *Guía del usuario de la utilidades de la controladora de administración de la placa base de Dell OpenManage* proporciona información adicional acerca de cómo usar Server Administrator para configurar y administrar la BMC del sistema.
- La *Guía del usuario de Dell EMC Server Administrator Storage Management* es una guía de referencia completa para la configuración y administración del almacenamiento local y remoto conectado a un sistema.
- *Guía del usuario de Racadm de Dell Remote Access Controller* proporciona información sobre el uso de la utilidad de línea de comando racadm.
- La *Guía del usuario de Dell Remote Controller* proporciona información completa sobre cómo instalar y configurar una controladora DRAC, y cómo usar un DRAC para acceder de manera remota a un sistema que no funciona.
- La *Guía del usuario de Dell Update Packages* proporciona información sobre cómo obtener y utilizar Dell Update Packages como parte de la estrategia de actualización del sistema.
- La *Guía del usuario de Dell EMC OpenManage Server Update Utility* proporciona información acerca de la obtención y el uso de la Server Update Utility (SUU) para actualizar los sistemas o para ver las actualizaciones disponibles para cualquier sistema que aparezca en el repositorio.
- La *Guía del usuario de Dell Management Console* ofrece información para instalar, configurar y utilizar la consola.
- La *Guía del usuario de Dell Lifecycle Controller)* brinda información sobre la configuración y el uso de Unified Server Configurator para ejecutar tareas de administración de sistemas y almacenamiento a lo largo de todo el ciclo de vida del sistema.
- La *Guía del usuario de Dell License Manager* proporciona información sobre cómo administrar licencias de servidor de componentes para los servidores de 12.ª generación.
- El *Glosario* proporciona información sobre los términos utilizados en este documento.

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

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

- Enlaces directos:

- Para Dell EMC Enterprise Systems Management y Dell EMC Remote Enterprise Systems Management:https://www.dell.com/esmmanuals
- Para Dell EMC Virtualization Solutions:https://www.dell.com/SoftwareManuals
- Para Dell EMC OpenManage:https://www.dell.com/openmanagemanuals
- Para iDRAC:https://www.dell.com/idracmanuals
- Para Dell EMC OpenManage Connections Enterprise Systems Management:https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Para Dell EMC Serviceability Tools:https://www.dell.com/serviceabilitytools

- Sitio de soporte de Dell EMC:
  1. Vaya a https://www.dell.com/support.
  2. Haga clic en **Examinar todos los productos**.
  3. En la página **Todos los productos**, haga clic en **Software** y, luego, haga clic en el enlace necesario.
  4. Haga clic en el producto necesario y, luego, haga clic en la versión necesaria.

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

Obtención de asistencia técnica

Si, en algún momento, no comprende un procedimiento descrito en esta guía, o bien si el producto no funciona correctamente, existen herramientas de ayuda disponibles. Para obtener más información sobre estas herramientas de ayuda, consulte **Obtener ayuda** en el *Manual del propietario de hardware* de su sistema.

Asimismo, hay disponibles formación y certificaciones para empresas; visite `dell.com/training` para obtener más información. Es posible que este servicio no esté disponible en todas las regiones.

Cómo ponerse en contacto con Dell EMC

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

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:

Vaya a **Dell.com/contactdell.**

2

Configuración y administración

Server Administrator proporciona seguridad a través del control de acceso basado en función (RBAC), de la autentificación y del cifrado tanto para la interfaz basada en web como para la interfaz de línea de comandos.

Temas:

Control de acceso basado en funciones

RBAC administra la seguridad mediante la determinación de las operaciones que pueden ejecutar las personas con funciones específicas. A cada usuario se le asigna una o más funciones y a cada función se le asigna uno o más privilegios que se les otorgan a los usuarios que tienen esa función. Con RBAC, la administración de la seguridad corresponde a la estructura de la organización.

Privilegios de usuario

Server Administrator otorga diferentes derechos de acceso según los privilegios de grupo asignados al usuario. Los cuatro niveles de privilegio del usuario son: Usuario, Usuario avanzado, Administrador y Administrador avanzado.

Tabla 2. Privilegios de usuario

Nivel de privilegio del usuario		Tipo de acceso		Descripción
	Ver		**Administrar**	
Usuario	Sí		No	Los *usuarios* pueden ver la mayor parte de la información.
Usuario avanzado	Sí		Sí	Los *usuarios avanzados* pueden establecer valores para los umbrales de aviso y configurar las acciones de alerta que se deberán realizar en caso de aviso o de error.
Administrador	Sí		Sí	Los *administradores* pueden configurar y realizar acciones de apagado, configurar acciones de recuperación automática, en caso de que un sistema tenga un sistema operativo que no responda, y borrar los registros de hardware, eventos y comandos. Los administradores también pueden configurar el sistema para que envíe correos electrónicos.
Administrador avanzado (solo en Linux)	Sí		Sí	Los *administradores avanzados* pueden ver y administrar información.

Niveles de privilegio para tener acceso a los servicios de Server Administrator

La siguiente tabla resume los usuarios que cuentan con privilegios para acceder a los servicios de Server Administrator y administrarlos.

Server Administrator otorga acceso de solo lectura a los usuarios conectados con privilegios de Usuario, acceso de lectura y escritura a los conectados con privilegios de Usuario avanzado, y acceso de lectura, escritura y administración a los usuarios conectados con privilegios de *Administrador* y *Administrador avanzado*.

Tabla 3. Privilegios necesarios para administrar los servicios de Server Administrator

Tabla 3. Privilegios necesarios para administrar los servicios de Server Administrator

Servicio	Nivel necesario de privilegio del usuario	
	Ver	**Administrar**
Instrumentación	Usuario, Usuario avanzado, Administrador y Administrador avanzado	Usuario avanzado, Administrador y Administrador avanzado
Acceso remoto	Usuario, Usuario avanzado, Administrador y Administrador avanzado	Administrador y Administrador avanzado
Storage Management	Usuario, Usuario avanzado, Administrador y Administrador avanzado	Administrador y Administrador avanzado

Autenticación

El esquema de autenticación de Server Administrator garantiza que se asignen los accesos correctos a los privilegios de usuario adecuados. Además, cuando se invoca la interfaz de línea de comandos (CLI), el esquema de autenticación de Server Administrator valida el contexto en el que se está ejecutando el proceso actual. Este esquema de autenticación garantiza que todas las funciones de Server Administrator, ya sea que se accedan mediante la página de inicio de Server Administrator o la CLI, se autentiquen adecuadamente.

Autentificación de Microsoft Windows

En los sistemas operativos Microsoft Windows admitidos, Server Administrator usa la autenticación de Windows integrada (anteriormente denominada NTLM) para autenticar. Este sistema de autenticación permite que la seguridad de Server Administrator se incorpore en un esquema de seguridad integral para la red.

Autenticación de Red Hat Enterprise Linux y SUSE Linux Enterprise Server

En los sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server compatibles, Server Administrator utiliza diversos métodos de autenticación según la biblioteca de módulos de autenticación conectables (PAM). Los usuarios pueden iniciar sesión en Server Administrator de forma local o remota mediante los protocolos de administración de cuentas diferentes, como LDAP, NIS, Kerberos y Winbind.

Autenticación de VMware ESXi Server

ESXi Server autentica a los usuarios que accedan a hosts ESXi mediante el cliente o el kit de desarrollo de software (SDK) de vSphere/VI. La instalación predeterminada de ESXi utiliza una base de datos de contraseñas local para la autenticación. Las transacciones de autenticación de ESXi con Server Administrator son también interacciones directas con el proceso **vmware-hostd**. Para garantizar que la autenticación funcione de forma eficiente para su sitio, efectúe tareas básicas como configurar usuarios, grupos, permisos, roles y atributos de usuario; agregar sus propios certificados, y determinar si desea usar SSL.

NOTA: En los sistemas que ejecuten el sistema operativo VMware ESXi Server, para iniciar sesión en Server Administrator todos los usuarios necesitan privilegios de administrador. Para obtener información sobre la asignación de roles, consulte la documentación de VMware.

Cifrado

El acceso a Server Administrator se realiza mediante una conexión HTTPS segura con tecnología de capa de sockets seguros (SSL) para garantizar y proteger la identidad del sistema administrado. Los sistemas operativos Microsoft Windows, Red Hat Enterprise Linux y SUSE Linux Enterprise Server admitidos utilizan Java Secure Socket Extension (JSSE) para proteger las credenciales de usuario y otros datos confidenciales que se transmiten a través de la conexión de sockets cuando los usuarios acceden a la página de inicio de **Server Administrator**.

Asignación de los privilegios de usuarios

Para garantizar la seguridad de los componentes críticos del sistema, antes de instalar el software OpenManage, asigne privilegios de usuario a todos los usuarios. Los nuevos usuarios pueden iniciar sesión en el software OpenManage utilizando los privilegios de usuario de su sistema operativo.

PRECAUCIÓN: Para proteger el acceso a los componentes críticos del sistema, asigne una contraseña a cada cuenta de usuario que pueda acceder al software OpenManage.

PRECAUCIÓN: Desactive las cuentas de invitados de los sistemas operativos Windows admitidos para proteger el acceso a los componentes críticos del sistema. Considere cambiar el nombre de las cuentas de invitados para que no sea posible habilitarlas mediante scripts remotos utilizando los nombres predeterminados de las cuentas de invitados.

NOTA: Para obtener instrucciones sobre cómo asignar privilegios de usuario en cada sistema operativo admitido, consulte la documentación del sistema operativo.

NOTA: Para agregar usuarios al software OpenManage, agregue nuevos usuarios al sistema operativo. No es necesario crear nuevos usuarios desde el software OpenManage.

Cómo agregar usuarios a un dominio en los sistemas operativos Windows

NOTA: Para realizar los siguientes procedimientos, debe tener Microsoft Active Directory instalado en el sistema. Consulte Uso del inicio de sesión de Active Directory para obtener más información sobre el uso de Active Directory.

1. Desplácese a **Panel de control** > **Herramientas administrativas** > **Usuarios y equipos de Active Directory**.
2. En el árbol de la consola, haga clic con el botón derecho del ratón en **Usuarios** o haga clic con el botón derecho del ratón en el contenedor en el que desea agregar al nuevo usuario y después apunte a **Nuevo** > **Usuario**.
3. Escriba la información de nombre de usuario adecuada en el cuadro de diálogo y haga clic en **Siguiente**.
4. Haga clic en **Siguiente** y, después, en **Terminar**.
5. Haga doble clic en el icono que representa al usuario que ha creado.
6. Haga clic en la ficha **Miembro de**.
7. Haga clic en **Agregar**.
8. Seleccione el grupo adecuado y haga clic en **Agregar**.
9. Haga clic en **Aceptar** y, después, haga clic en **Aceptar** otra vez.

   NOTA: Los nuevos usuarios pueden iniciar sesión en OpenManage con los privilegios de usuario de su dominio y grupo asignados.

Creación de usuarios de Server Administrator para sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server admitidos

Los privilegios de acceso de administrador se asignan al usuario que inició sesión como root. Para obtener información acerca de la creación de usuarios y grupos de usuarios, consulte la documentación del sistema operativo.

NOTA: Para realizar los siguientes procedimientos debe iniciar sesión como usuario `root` o equivalente.

NOTA: Para realizar los procedimientos debe tener la utilidad **useradd** instalada en el sistema.

Enlaces relacionados:

- Creación de usuarios con privilegios de usuario
- Creación de usuarios con privilegios de usuario avanzado

Creación de usuarios con privilegios de usuario

1. Ejecute el siguiente comando en la línea de comandos: `useradd -d <home-directory> -g <group> <username>` donde `<group>` no es `root`.

   NOTA: Si `<group>` no existe, debe crearlo mediante el comando **groupadd**.

2. Escriba `passwd <username>` y presione <Intro>.
3. Cuando se le solicite, ingrese la contraseña para el nuevo usuario.

   NOTA: Asigne una contraseña a cada cuenta de usuario que pueda acceder a Server Administrator para proteger el acceso a componentes críticos del sistema.

   El nuevo usuario puede iniciar sesión en Server Administrator con privilegios de grupo de usuarios.

Creación de usuarios con privilegios de usuario avanzado

1. Ejecute el siguiente comando en la línea de comandos:`useradd -d <home-directory> -g <group> <username>`

   NOTA: Establezca `root` como el grupo principal.

2. Escriba `passwd <username>` y presione <Intro>.
3. Cuando se le solicite, ingrese la contraseña para el nuevo usuario.

   NOTA: Asigne una contraseña a cada cuenta de usuario que pueda acceder a Server Administrator para proteger el acceso a componentes críticos del sistema.

   El nuevo usuario puede iniciar sesión en Server Administrator con privilegios de grupo de usuarios avanzados.

Modificación de los privilegios de usuario de Server Administrator en los sistemas operativos Linux

NOTA: Debe iniciar sesión como usuario raíz o equivalente.

1. Abra el archivo **omarolemap** en `/opt/dell/srvadmin/etc/omarolemap`.
2. Agregue la siguiente información en el archivo: `<User_Name>[Tab]<Host_Name>[Tab]<Rights>`

   La siguiente tabla enumera la leyenda para agregar la definición de roles a **omarolemap.**

Tabla 4. Leyenda para agregar la definición de funciones en Server Administrator

<User_Name>	<Host_Name>	<Rights>
Username	Nombre del host	Administrador
(+) Nombre de grupo	Dominio	Usuario
Comodín (*)	Comodín (*)	Usuario
`[Tab] = \t (tab character)`		

La siguiente tabla enumera ejemplos para agregar la definición de roles al archivo **omarolemap** .

Tabla 5. Ejemplos para agregar la definición de funciones en Server Administrator

<User_Name>	<Host_Name>	<Rights>
Roberto	Ahost	Usuario avanzado
+ root	Bhost	Administrador
+ root	Chost	Administrador
Roberto	*.aus.amer.com	Usuario avanzado

Tabla 5. Ejemplos para agregar la definición de funciones en Server Administrator

<User_Name>	<Host_Name>	<Rights>
Miguel	192.168.2.3	Usuario avanzado

3. Guarde y cierre el archivo.

Recomendaciones de uso del archivo omarolemap

A continuación se muestran las sugerencias para tener en cuenta cuando trabaje con **omarolemap**:

- No elimine las anotaciones predeterminadas siguientes dentro del archivo **omarolemap**.

Tabla 6. Recomendaciones de uso para el archivo omarolemap

root	Administrador
+root	* Poweruser
*	* User

- No cambie los permisos de archivo ni el formato del archivo **omarolemap**.
- No utilice la dirección de bucle cerrado para *<Host_Name>*, por ejemplo, localhost o 127.0.0.1.
- Una vez que los servicios de conexión se reinicien, si los cambios no tienen efecto para el archivo **omarolemap**, consulte el registro de comandos para determinar si hay errores.
- Al copiar el archivo **omarolemap** de una máquina a otra, los permisos de archivo y las anotaciones del archivo se deben volver a revisar.
- Preceda el *Group Name* con un signo *+*.
- Server Administrator utiliza los privilegios de usuario predeterminados del sistema operativo si:
  - un usuario se degrada en el archivo **omarolemap**
  - existen entradas duplicadas de nombres de usuario o grupos de usuarios con el mismo *<Host_Name>*
- También puede utilizar `Space` como delimitador de columnas en lugar de `[Tab]`.

Creación de usuarios de Server Administrator para VMware ESXi 6.*X*

Para agregar un usuario a la tabla Usuarios:

1. Inicie sesión en el host por medio de vSphere Client.
2. Haga clic en la ficha **Usuarios y grupos** y, después, en **Usuarios**.
3. Haga clic con el botón derecho del mouse en cualquier parte de la tabla Usuarios y después en **Agregar** para abrir el cuadro de diálogo **Agregar nuevo usuario**.
4. Introduzca el inicio de sesión, el nombre de usuario, una id. de usuario numérica (UID) y la contraseña, y especifique que el nombre de usuario y la UID son opcionales. Si no especifica la UID, el cliente de vSphere asigna la siguiente UID disponible.
5. Para permitir a un usuario acceder al host de ESXi a través de un shell de comandos, seleccione **Otorgar acceso de shell a este usuario**. Los usuarios que accedan al host solo a través del cliente de vSphere no necesitan acceso de shell.
6. Para agregar el usuario a un grupo, seleccione el nombre del grupo en el menú desplegable **Grupo** y haga clic en **Agregar**.
7. Haga clic en **Aceptar**.

Desactivación de cuentas anónimas y de invitados en sistemas operativos Windows compatibles

NOTA: Debe iniciar sesión con privilegios de administrador.

1. Abra la ventana **Administración del equipo**.
2. En el árbol de la consola, expanda **Usuarios locales y grupos** y haga clic en **Usuarios**.
3. Haga doble clic en **Invitado** o en la cuenta de usuario **IUSR_system** para ver las propiedades de esos usuarios, o bien, haga clic con el botón derecho del mouse en **Invitado** o en la cuenta de usuario **IUSR_***system* y seleccione la opción **Propiedades**.
4. Seleccione **Cuenta desactivada** y haga clic en **Aceptar**.
   Un círculo rojo con una X aparece en el nombre de usuario para indicar que la cuenta está desactivada.

Configuración del agente SNMP

Server Administrator admite el protocolo simple de administración de redes (SNMP, un estándar de administración de sistemas) en todos los sistemas operativos compatibles. La compatibilidad de SNMP puede estar instalada o no en función del sistema operativo y la forma en la que se instaló. En la mayoría de los casos, el SNMP se instala junto con el sistema operativo. Se requiere un estándar de protocolo de administración de sistemas admitido instalado, como el SNMP, para poder instalar Server Administrator.

Se puede configurar el agente SNMP para cambiar el nombre de la comunidad y enviar capturas a una estación de administración. Para configurar el agente SNMP para lograr una interacción adecuada con las aplicaciones de administración como OpenManage Essentials, realice los procedimientos descritos en las siguientes secciones.

NOTA: La configuración predeterminada del agente SNMP generalmente incluye un nombre de comunidad para el SNMP, como "público". Por razones de seguridad, debe cambiar los nombres de comunidad predeterminados del SNMP. Para obtener información acerca de cómo cambiar los nombres de comunidad SNMP, consulte Cambio del nombre de comunidad SNMP.

NOTA: Para que OpenManage Essentials pueda recuperar la información de administración de un sistema que ejecuta Server Administrator, el nombre de comunidad utilizado por OpenManage Essentials debe coincidir con un nombre de comunidad del sistema que ejecuta Server Administrator. Para que OpenManage Essentials modifique información o realice acciones en un sistema que ejecute Server Administrator, el nombre de la comunidad utilizado por OpenManage Essentials debe coincidir con un nombre de comunidad que permita operaciones Set en el sistema que ejecuta Server Administrator. Para que OpenManage Essentials reciba capturas (notificaciones de eventos asíncronos) de un sistema que ejecuta Server Administrator, el sistema que ejecuta Server Administrator debe estar configurado para el envío de capturas al sistema que ejecuta OpenManage Essentials.

Los siguientes procedimientos proporcionan instrucciones paso a paso para configurar el agente SNMP para cada sistema operativo compatible:

- Configuración del agente SNMP en sistemas que ejecutan sistemas operativos Windows compatibles
- Configuración del agente SNMP en sistemas que ejecutan Red Hat Enterprise Linux compatible
- Configuración del agente SNMP en sistemas que ejecutan SUSE Linux Enterprise Server admitido
- Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESXi 5.X y ESXi 6.X admitidos
- Configuración del agente SNMP en sistemas que ejecutan Ubuntu Server compatible

Configuración del agente SNMP en sistemas que ejecutan sistemas operativos Windows compatibles

Server Administrator utiliza los servicios SNMP que el agente SNMP de Windows proporciona. Puede configurar el agente SNMP para cambiar el nombre de la comunidad y enviar capturas a una estación de administración. Para configurar el agente SNMP para lograr una interacción adecuada con las aplicaciones de administración como OpenManage Essentials, realice los procedimientos que se describen en las siguientes secciones.

NOTA: Para obtener más información sobre la configuración de SNMP, consulte la documentación del sistema operativo.

Cambio del nombre de comunidad SNMP

NOTA: No puede establecer el nombre de comunidad SNMP desde Server Administrator. Establezca el nombre de comunidad con las herramientas SNMP del sistema operativo.

Al configurar los nombres de comunidad SNMP es posible determinar qué sistemas pueden administrar el sistema a través de SNMP. El nombre de comunidad SNMP que utilizan las aplicaciones de administración debe coincidir con un nombre de comunidad SNMP que esté configurado en el sistema que ejecuta Server Administrator, de modo tal que las aplicaciones de administración puedan recuperar la información de administración desde Server Administrator.

1. Abra la ventana **Administración del equipo**.
2. Si es necesario, expanda el icono **Administración del equipo** que aparece en la ventana.
3. Expanda el icono **Servicios y aplicaciones** y haga clic en **Servicios**.
4. Desplácese hacia abajo en la lista de servicios hasta encontrar **Servicio SNMP**, haga clic con el botón derecho del mouse en **Servicio SNMP** y, a continuación, haga clic en **Propiedades**.

   Se desactiva la ventana **Propiedades del servicio SNMP**.
5. Haga clic en la ficha **Seguridad** para agregar o editar un nombre de comunidad.

Para agregar un nombre de comunidad:

a. Haga clic en **Agregar** en la lista **Nombres de comunidad aceptados**.

   Aparece la ventana **Configuración del servicio SNMP**.

b. Escriba el nombre de comunidad de un sistema que pueda administrar su sistema (el valor predeterminado es **public**) en el cuadro de texto **Nombre de comunidad** y haga clic en Agregar.

   Aparece la ventana **Propiedades del servicio SNMP**.

Para editar un nombre de comunidad:

a. Seleccione un nombre de comunidad en la lista **Nombres de comunidad aceptados** y haga clic en **Editar**.

   Aparece la ventana **Configuración del servicio SNMP**.

b. Edite el nombre de comunidad en la casilla **Nombre de comunidad** y, a continuación, haga clic en **Aceptar**.

   Aparece la ventana **Propiedades del servicio SNMP**.

6. Haga clic en **Aceptar** para guardar los cambios.

Configuración del sistema para enviar capturas SNMP a una estación de administración

Server Administrator genera capturas SNMP en respuesta a los cambios en el estado de los sensores y a otros parámetros supervisados. Se deben configurar uno o varios destinos de captura en el sistema que ejecuta Server Administrator para enviar capturas SNMP a una estación de administración.

1. Abra la ventana **Administración de la computadora**.
2. Si es necesario, expanda el ícono **Administración de la computadora** que aparece en la ventana.
3. Expanda el ícono **Servicios y aplicaciones** y haga clic en **Servicios**.
4. Desplácese hacia abajo en la lista de servicios hasta encontrar **Servicio SNMP**, haga clic con el botón derecho del mouse en **Servicio SNMP** y, a continuación, haga clic en **Propiedades**.

   Aparecerá la ventana **Propiedades del servicio SNMP**.

5. Haga clic en la ficha **Capturas** para agregar una comunidad para las capturas o un destino de captura para una comunidad de capturas.
   a. Para agregar una comunidad para capturas, escriba el nombre de la comunidad en el cuadro **Nombre de comunidad** y haga clic en **Agregar a la lista**, que se encuentra al lado del cuadro **Nombre de comunidad**.
   b. Para agregar un destino de captura para una comunidad de capturas, seleccione el nombre de la comunidad en el cuadro despegable **Nombre de comunidad** y haga clic en **Agregar** en el cuadro **Destinos de captura**.

      Aparecerá la ventana **Configuración del servicio SNMP**.

   c. En el **Hostname**, **cuadro de dirección IP o IPX**, escriba el destino de captura, **Agregar**.

      Aparecerá la ventana **Propiedades del servicio SNMP**.

6. Haga clic en **Aceptar** para guardar los cambios.

Configuración del agente SNMP en sistemas que ejecutan Red Hat Enterprise Linux compatible

Server Administrator utiliza los servicios SNMP que el agente SNMP **net-snmp** proporciona. Puede configurar el agente SNMP para cambiar el nombre de la comunidad y enviar capturas a una estación de administración. Para configurar el agente SNMP para lograr una interacción adecuada con las aplicaciones de administración como OpenManage Essentials, realice los procedimientos que se describen en las siguientes secciones.

NOTA: Para obtener más información sobre la configuración de SNMP, consulte la documentación del sistema operativo.

Configuración del control de acceso para el agente SNMP

El identificador del objeto (OID) 1.3.6.1.4.1.674 reconoce la rama de la base de información de administración (MIB) que implementa Server Administrator. Las aplicaciones de administración deben tener acceso a esta rama del árbol de MIB para administrar los sistemas que ejecutan Server Administrator.

Para sistemas operativos Red Hat Enterprise Linux y VMware ESXi, la configuración predeterminada del agente SNMP proporciona acceso de sólo lectura para la comunidad *pública* solo a la rama del sistema MIB-II (identificada por OID 1.3.6.1.2.1.1) del árbol de MIB. Esta configuración no permite que las aplicaciones de administración puedan recuperar o cambiar Server Administrator ni otra información de administración de sistemas fuera de la rama de *sistema* MIB-II.

Acciones de instalación del agente SNMP de Server Administrator

Si Server Administrator detecta la configuración de SNMP predeterminada durante la instalación, intenta modificar la configuración del agente SNMP para proporcionar acceso de solo lectura al árbol de MIB completo para la comunidad public. Server Administrator modifica el archivo de configuración del agente SNMP `/etc/snmp/snmpd.conf` de la siguiente forma:

- Crea una vista del árbol de MIB completo mediante la siguiente línea, si no existe: `view all included`
- Modifica la línea de acceso predeterminada para proporcionar acceso de solo lectura al árbol de MIB completo para la comunidad public. Server Administrator busca la siguiente línea: `access notConfigGroup "" any noauth exact systemview none none`
- Si Server Administrator encuentra la línea mencionada anteriormente, la modifica de la siguiente manera: `access notConfigGroup "" any noauth exact all none none`

  NOTA: Para asegurar que Server Administrator pueda modificar la configuración del agente SNMP para proporcionar acceso correcto a los datos de Systems Management, se recomienda hacer cualquier otro cambio a la configuración del agente SNMP después de instalar Server Administrator.

SNMP de Server Administrator se comunica con el agente SNMP mediante el protocolo de multiplexación de SNMP (SMUX). Cuando SNMP de Server Administrator se conecta con el agente SNMP, envía un identificador del objeto a un agente SNMP para identificarse como un sistema SMUX del mismo nivel. Dado que ese identificador de objeto debe estar configurado con el agente SNMP, Server Administrator agrega la siguiente línea al archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf`, durante la instalación, si no existe:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Cambio del nombre de comunidad SNMP

Al configurar el nombre de la comunidad SNMP es posible determinar qué sistemas pueden administrar el sistema a través de SNMP. El nombre de comunidad SNMP que utilizan las aplicaciones de administración debe coincidir con un nombre de comunidad SNMP que esté configurado en el sistema que ejecuta Server Administrator, de modo tal que las aplicaciones de administración puedan recuperar la información de administración desde Server Administrator.

Para cambiar el nombre de comunidad SNMP que se utiliza para recuperar la información de administración de un sistema que ejecuta Server Administrator:

1. Abra el archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf`.
2. Busque la línea que dice: `com2sec publicsec default public` o `com2sec notConfigUser default public`.

   NOTA: En el caso de IPv6, busque la línea `com2sec6 notConfigUser default public`. Asimismo, agregue el texto `agentaddress udp6:161` en el archivo.

3. Edite esta línea, reemplazando `public` con el nuevo nombre de comunidad SNMP. Una vez editada, la nueva línea debe decir: `com2sec publicsec default community_name` o `com2sec notConfigUser default community_name`.
4. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP. Para eso, escriba: `systemctl restart snmpd .`

Configuración del sistema para enviar capturas a una estación de administración

Server Administrator genera capturas SNMP en respuesta a los cambios en el estado de los sensores y a otros parámetros supervisados. Se deben configurar uno o varios destinos de captura en el sistema que ejecuta Server Administrator para enviar capturas SNMP a una estación de administración.

Para configurar el sistema que ejecuta Server Administrator para que envíe capturas a una estación de administración, edite el archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf` y realice los pasos siguientes:

1. Agregue la línea siguiente al archivo: `trapsink IP_address community_name`, donde `IP_address` es la dirección IP de la estación de administración y `community_name` es el nombre de comunidad SNMP.
2. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP. Para eso, escriba: `systemctl restart snmpd .`

Configuración del agente SNMP en sistemas que ejecutan un SUSE Linux Enterprise Server admitido

Server Administrator usa los servicios SNMP proporcionados por el agente net-snmp. Puede configurar el agente SNMP para permitir el acceso a SNMP desde hosts remotos, para cambiar el nombre de comunidad, para activar operaciones Set y para enviar capturas a una estación de administración. Para configurar el agente SNMP para lograr una interacción adecuada con las aplicaciones de administración como OpenManage Essentials, realice los procedimientos que se describen en las siguientes secciones.

NOTA: Para obtener más información sobre la configuración de SNMP, consulte la documentación del sistema operativo.

Acciones de instalación de SNMP de Server Administrator

SNMP de Server Administrator se comunica con el agente SNMP mediante el protocolo SMUX. Cuando SNMP de Server Administrator se conecta con el agente SNMP, envía un identificador del objeto a un agente SNMP para identificarse como un sistema SMUX del mismo nivel. Como el identificador de objeto debe configurarse con el agente SNMP, Server Administrator agrega la siguiente línea al archivo de configuración del agente SNMP, **/etc/snmp/snmpd.conf**, durante la instalación, si esta no existe:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Activación del acceso a SNMP desde hosts remotos

La configuración predeterminada del agente SNMP en los sistemas operativos SUSE Linux Enterprise Server otorga acceso de solo lectura al árbol completo de la MIB para la comunidad public desde el host local solamente. Esta configuración no permite que las aplicaciones de administración de SNMP como OpenManage Essentials se ejecuten en otros hosts para descubrir y administrar correctamente los sistemas de Server Administrator. Si Server Administrator detecta esta configuración durante la instalación, registra un mensaje en el archivo de registro del sistema operativo, `/var/log/messages`, para indicar que el acceso de SNMP está restringido para el host local. Debe configurar el agente SNMP para activar el acceso de SNMP desde hosts remotos si planea administrar el sistema mediante aplicaciones de administración de SNMP desde hosts remotos.

NOTA: Por motivos de seguridad, se recomienda restringir el acceso a SNMP a hosts remotos específicos, si es posible.

Para activar el acceso a SNMP desde un host remoto específico a un sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf`, y realice los siguientes pasos:

1. Busque la línea que dice: . `rocommunity public 127.0.0.1`.
2. Edite o copie esta línea, reemplace 127.0.0.1 por la dirección IP de host. Una vez editada, la nueva línea debe decir: `rocommunity public IP_address`.

   NOTA: Puede activar el acceso a SNMP desde varios hosts remotos específicos mediante una directiva `rocommunity` para cada host remoto.

3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP. Para eso, escriba: `systemctl restart snmpd .`

Cambio del nombre de comunidad SNMP

Configurar el nombre de comunidad SNMP determina qué estaciones de administración pueden administrar el sistema mediante SNMP. El nombre de comunidad SNMP que utilizan las aplicaciones de administración debe coincidir con el nombre de comunidad SNMP configurado en el sistema que ejecuta Server Administrator, de tal modo que las aplicaciones de administración puedan recuperar la información de administración desde Server Administrator.

Para cambiar el nombre predeterminado de la comunidad SNMP utilizado para recuperar la información de administración de un sistema que ejecuta Server Administrator:

1. Abra el archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf`.
2. Busque la línea que dice: `rocommunity public 127.0.0.1.`
3. Edite esta línea mediante la sustitución de `public` por el nuevo nombre de comunidad SNMP. Una vez editada, la nueva línea debe decir: `rocommunity community_name 127.0.0.1.`
4. Para activar los cambios en la configuración de SNMP, escriba para reiniciar el agente SNMP: `systemctl restart snmpd .`

Configuración del agente SNMP en sistemas que ejecutan Ubuntu Server compatible

Server Administrator usa los servicios SNMP proporcionados por el agente net-snmp. Se puede configurar el agente SNMP para permitir el acceso a SNMP desde hosts remotos, para cambiar el nombre de comunidad y para enviar capturas a una estación de administración. Para configurar el agente SNMP para lograr una interacción adecuada con las aplicaciones de administración como OpenManage Essentials, realice los procedimientos que se describen en las siguientes secciones.

NOTA: Para obtener más información sobre la configuración de SNMP, consulte la documentación del sistema operativo.

Acciones de instalación de SNMP de Server Administrator

SNMP de Server Administrator se comunica con el agente SNMP mediante el protocolo SMUX. Cuando SNMP de Server Administrator se conecta con el agente SNMP, envía un identificador del objeto a un agente SNMP para identificarse como un sistema SMUX del mismo nivel. Para admitir SMUX este identificador de objeto se debe configurar con el agente SNMP. Para que Server Administrator trabaje con el protocolo SMUX, necesita activarlo mediante los siguientes pasos en el archivo de configuración del agente SNMP.

- Abra el archivo de configuración del agente SNMP. `/etc/default/snmpd`.
- La opción predeterminada disponible en el archivo de configuración es: `SNMPDOPTS= ' -Lsd -Lf /dev/null -u -g snmp snmp -I -smux,mteTrigger,mteTriggerConf -p /run/snmpd.pid'`
- Con la configuración predeterminada anterior se desactiva el módulo SMUX.
- Para admitir que snmpd admita SMUX, cambie la configuración así: `SNMPDOPTS= ' -Lsd -Lf /dev/null snmp -g -u -p snmp /run/snmpd.pid'`

Agregue en el archivo de configuración del agente SNMP . `/etc/snmp/snmpd.conf`

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

- Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP mediante: `systemctl restart snmpd`.

Cambio del nombre de comunidad SNMP

Configurar el nombre de comunidad SNMP determina qué estaciones de administración pueden administrar el sistema mediante SNMP. El nombre de comunidad SNMP que utilizan las aplicaciones de administración debe coincidir con el nombre de comunidad SNMP configurado en el sistema que ejecuta Server Administrator, de tal modo que las aplicaciones de administración puedan recuperar la información de administración desde Server Administrator.

Para cambiar el nombre predeterminado de la comunidad SNMP utilizado para recuperar la información de administración de un sistema que ejecuta Server Administrator:

1. Abra el archivo de configuración del agente SNMP, `/etc/snmp/snmpd.conf`.
2. Busque la línea que dice: `rocommunity public 127.0.0.1.`
3. Edite esta línea mediante la sustitución de `public` por el nuevo nombre de comunidad SNMP. Una vez editada, la nueva línea debe decir: `rocommunity community_name 127.0.0.1.`
4. Para activar los cambios en la configuración de SNMP, escriba para reiniciar el agente SNMP: `systemctl restart snmpd .`

Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESXi 6.X admitidos

Server Administrator admite las capturas SNMP en VMWare ESXi 6.X. Si solo hay una licencia independiente, la configuración de SNMP fallará en los sistemas operativos VMware ESXi. Server Administrator no admite las operaciones Get y Set de SNMP en VMWare ESXi 6.X ya que la compatibilidad necesaria con SNMP no está disponible. La interfaz de línea de comandos (CLI) de VMware vSphere se utiliza para configurar sistemas que ejecutan VMware ESXi 6.X para enviar capturas SNMP a una estación de administración.

NOTA: Para obtener más información sobre cómo utilizar la CLI de VMware vSphere, consulte **vmware.com/support**.

Configuración del sistema para enviar capturas a una estación de administración

Server Administrator genera capturas SNMP en respuesta a los cambios en el estado de los sensores y a otros parámetros supervisados. Se deben configurar uno o varios destinos de captura en el sistema que ejecuta Server Administrator para enviar capturas SNMP a una estación de administración.

Para configurar el sistema ESXi que ejecuta Server Administrator para enviar capturas a una estación de administración:

1. Instale la CLI de VMware vSphere.
2. Abra un indicador de comandos en el sistema donde está instalada la CLI de VMware vSphere.
3. Cambie al directorio en el cual esté instalada la CLI de VMware vSphere. La ubicación predeterminada en Linux es `/usr/bin`. La ubicación predeterminada en Windows es `C:\Program Files\VMware\VMware vSphere CLI\bin`.
4. Ejecute el siguiente comando: `vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname> @162/<community>`

   donde `<server>` es el hostname o la dirección IP del sistema ESXi, `<username>` es un usuario en el sistema ESXi, `<community>` es el nombre de la comunidad SNMP y `<hostname>` es el hostname o la dirección IP de la estación de administración.

   NOTA: La extensión .pl no es necesaria en Linux.

   NOTA: Si no especifica un nombre de usuario y una contraseña, se le solicitará.

La configuración de capturas SNMP tiene efecto de manera inmediata sin reiniciar los servicios.

Configuración de firewall en sistemas que ejecutan sistemas operativos compatibles Red Hat Enterprise Linux y SUSE Linux Enterprise Server

Si activa la seguridad del firewall durante la instalación de Red Hat Enterprise Linux/SUSE Linux, el puerto SNMP se cierra de manera predeterminada en todas las interfaces de red externas. Para permitir que las aplicaciones de administración de SNMP, como OpenManage Essentials, descubran y recuperen información en Server Administrator, el puerto SNMP debe estar abierto en al menos una interfaz de red externa. Si Server Administrator detecta que el puerto SNMP no está abierto en el firewall para cualquier interfaz de red externa, Server Administrator muestra un mensaje de advertencia y registra un mensaje en el registro del sistema.

Puede abrir el puerto SNMP mediante la desactivación del firewall, la apertura de una interfaz de red externa en el firewall o la apertura del puerto SNMP para al menos una interfaz de red externa en el firewall. Puede realizar esta acción antes o después de iniciar Server Administrator.

Para abrir el puerto SNMP en Red Hat Enterprise Linux mediante uno de los métodos descritos anteriormente:

1. En el símbolo del sistema de Red Hat Enterprise Linux, escriba `setup` y presione <Intro> para iniciar la utilidad de configuración de modo de texto.

   NOTA: Este comando está disponible solo si ha realizado la instalación predeterminada del sistema operativo.

   Aparecerá el menú de **Elegir una herramienta**.
2. Seleccione **Configuración de firewall** mediante la flecha hacia abajo y presione <Intro>.
   Aparecerá la pantalla **Configuración de firewall**.
3. Presione <Tab> para seleccionar **Nivel de seguridad** y, a continuación, presione la barra espaciadora para seleccionar el nivel de seguridad que desea establecer. El **Nivel de seguridad** seleccionado se indica con un asterisco.

   NOTA: Para obtener más información sobre los niveles de seguridad del firewall, presione <F1>. El número predeterminado de puerto SNMP es 161. Si utiliza la interfaz gráfica de usuario del sistema X Window, es posible que al presionar <F1> no se proporcione información sobre los niveles de seguridad del firewall en las versiones más recientes de Red Hat Enterprise Linux.

   a. Para desactivar el firewall, seleccione **Sin firewall** o **Desactivado** y vaya al paso 7.
   b. Para abrir una interfaz de red completa o el puerto SNMP, seleccione **Alto, Medio** o **Activado** y continúe con el paso 4.
4. Presione <Tab> para ir a Personalizar y presione <Intro>.

   Aparecerá la pantalla **Configuración del firewall: Personalizar**.
5. Seleccione si desea abrir una interfaz de red completa o solo el puerto SNMP en todas las interfaces de red.

a. Para abrir una interfaz de red completa, presione <Tab> para ir a uno de los dispositivos de confianza y presione la barra espaciadora. Un asterisco en el cuadro a la izquierda del nombre del dispositivo indica que la interfaz completa está abierta.
b. Para abrir el puerto SNMP en todas las interfaces de red, presione <Tab> para ir a Otros puertos y escriba `snmp:udp`.

6. Presione <**Tab**> para seleccionar **Aceptar** y presione <**Intro**>
Aparecerá la pantalla **Configuración de firewall**.
7. Presione <**Tab**> para seleccionar **Aceptar** y presione <**Intro**>
Aparecerá el menú de **Elegir una herramienta**.
8. Presione <**Tab**> para seleccionar **Salir** y presione <**Intro**>.

Configuración del servidor de seguridad

Para abrir el puerto SNMP en SUSE Linux Enterprise Server:

1. Configure SuSEfirewall2 mediante la ejecución del siguiente comando en una consola: `a.# yast2 firewall`
2. Utilice las teclas de flecha para acceder a **Servicios admitidos**.
3. Presione <Alt><d> para abrir el cuadro de diálogo **Puertos admitidos adicionales**.
4. Presione <Alt><T> para desplazar el cursor al cuadro de texto **Puertos TCP**.
5. Escriba **snmp** en el cuadro de texto.
6. Presione la tecla <Alt><O> <Alt><N> para ir a la siguiente pantalla.
7. Presione la tecla <Alt><A> para aceptar y aplicar los cambios.

3

Uso de Server Administrator

Para iniciar una sesión de Server Administrator, haga doble clic en el icono **Server Administrator** del escritorio.

Aparecerá la pantalla **Inicio de sesión en Server Administrator**. El puerto predeterminado para Server Administrator es 1311. Si es necesario, puede cambiar el puerto. Para obtener instrucciones acerca de cómo configurar las preferencias del sistema, consulte Servicio de conexión y configuración de seguridad de la administración de servidores de Systems Management.

Temas:

Inicio y cierre de sesión

Server Administrator ofrece los siguientes tipos de inicio de sesión:

- Inicio de sesión en el sistema local de Server Administrator
- Inicio de sesión en el sistema administrado de Server Administrator: uso del icono de escritorio
- Inicio de sesión en el sistema administrado de Server Administrator: uso del explorador web
- Inicio de sesión en Central Web Server

Inicio de sesión en el sistema local de Server Administrator

El inicio de sesión en el sistema local de Server Administrator solo está disponible si los componentes de Server Instrumentation y Web Server de Server Administrator están instalados en el sistema local.

NOTA: El inicio de sesión en el sistema local de Server Administrator no está disponible para los servidores que ejecutan XenServer 6.5.

Para iniciar sesión en Server Administrator en un sistema local:

1. Escriba el **nombre de usuario** y la **contraseña** asignados previamente en los campos correspondientes de la ventana **Conectar** de Systems Management.

   Si accede a Server Administrator desde un dominio definido, también debe especificar el nombre de dominio correcto.

2. Seleccione la casilla **Inicio de sesión de Active Directory** para iniciar sesión por medio de Microsoft Active Directory. Consulte Uso del inicio de sesión de Active Directory.
3. Haga clic en **Enviar**.

Para finalizar la sesión de Server Administrator, haga clic en el botón **Cerrar sesión** que se encuentra en la esquina superior derecha de cada página de inicio de **Server Administrator**.

NOTA: Para obtener información sobre la configuración de Active Directory en sistemas que utilizan CLI, consulte la *Guía de instalación del software Management Station* en `dell.com/openmanagemanuals`.

Inicio de sesión en el sistema administrado de Server Administrator: uso del icono de escritorio

Esta forma de inicio de sesión solo se encuentra disponible si el componente Server Administrator Web Server está instalado en el sistema. Para iniciar sesión en Server Administrator para administrar un sistema remoto:

1. Haga doble clic en el icono **Server Administrator** del escritorio.
2. Escriba la dirección IP o nombre del sistema o nombre de dominio completo (FQDN) del sistema administrado.

   NOTA: Si ha introducido el nombre del sistema o FQDN, el host de Server Administrator Web Server convierte el nombre del sistema o FQDN en la dirección IP de Managed System. También se puede conectar introduciendo el número de puerto del sistema administrado en el siguiente formato: nombre del host:número de puerto o dirección IP:número de puerto.

3. Si va a utilizar una conexión de Intranet, seleccione **Ignorar advertencias de certificado**.
4. Seleccione **Inicio de sesión de Active Directory** para iniciar sesión por medio de la autenticación de Microsoft Active Directory. Si el software de Active Directory no se utiliza para controlar el acceso a la red, no seleccione **Inicio de sesión de Active Directory**. Consulte Uso del inicio de sesión de Active Directory.
5. Haga clic en **Enviar.**

Inicio de sesión en el sistema administrado de Server Administrator: uso del explorador web

NOTA: Debe contar con derechos de usuario previamente asignados para iniciar sesión en Server Administrator. Consulte Configuración y administración para obtener instrucciones acerca de la configuración de usuarios nuevos.

1. Abra el explorador web.
2. En el campo Dirección, escriba una de las siguientes:
   - `https://hostname:1311`, donde hostname es el nombre asignado para el sistema administrado y 1311 es el número de puerto predeterminado.
   - `https://IP address:1311`, donde IP address es la dirección IP para el sistema administrado y 1311 es el número de puerto predeterminado.

   NOTA: Asegúrese de escribir `https://` (y no `http://`) en el campo de dirección.

3. Presione <Intro>.

Inicio de sesión en Central Web Server

Esta forma de inicio de sesión solo se encuentra disponible si el componente Server Administrator Web Server está instalado en el sistema. Utilice este inicio de sesión para administrar Server Administrator Central Web Server:

1. Haga doble clic en el icono **Server Administrator** del escritorio. Se visualiza la página de inicio de sesión remoto.

   PRECAUCIÓN: La pantalla de inicio de sesión muestra la casilla de verificación Ignorar avisos de certificado. Debe utilizar esta opción con prudencia. Se recomienda que la utilice solamente en entornos de Intranet de confianza.

2. Haga clic en el vínculo **Administrar Web Server**, ubicado en la esquina superior derecha de la pantalla.
3. Introduzca **el nombre de usuario, la contraseña** y **el nombre de dominio** (si accede a Server Administrator desde un dominio definido) y haga clic en **Enviar**.
4. Seleccione **Inicio de sesión de Active Directory** para iniciar sesión por medio de Microsoft Active Directory. Consulte Uso del inicio de sesión de Active Directory.
5. Haga clic en **Enviar**.

   Para cerrar la sesión de Server Administrator, haga clic en **Cerrar sesión** en la Barra de navegación global.

   NOTA: Al iniciar Server Administrator con Mozilla Firefox o Microsoft Internet Explorer, es posible que aparezca una página intermediaria de advertencia para indicar un problema con el certificado de seguridad. Para garantizar la seguridad del sistema, se le recomienda generar un certificado X.509 nuevo, volver a usar un certificado X.509 existente o importar una cadena de certificados de una entidad de certificación (CA). Para evitar tales mensajes de advertencia sobre el certificado, el certificado utilizado debe usarse desde una CA de confianza. Para obtener más información sobre la administración de certificados X.509, consulte Administración de certificados X. 509.

   NOTA: Para garantizar la seguridad del sistema, se recomienda que importe una cadena de certificados de una entidad de certificación (CA). Para obtener más información, consulte la documentación de VMware.

NOTA: Si la entidad de certificación del sistema administrado es válida y el servidor web de Server Administrator todavía indica un error de certificado no fiable, puede hacer que la CA del sistema administrado sea fiable mediante el archivo `certutil.exe`. Para obtener información sobre cómo acceder a este archivo .exe, consulte la documentación del sistema operativo. En los sistemas operativos Windows compatibles, también puede utilizar la opción de complemento de certificados para importar certificados.

Uso del inicio de sesión de Active Directory

Debe seleccionar **Inicio de sesión de Active Directory** para conectarse por medio de Dell Extended Schema Solution en Active Directory.

Esta solución permite otorgar acceso a Server Administrator; lo cual permite agregar y controlar usuarios y privilegios de Server Administrator a usuarios existentes en el software de Active Directory. Para obtener más información, consulte Uso de Microsoft Active Directory en la *Guía de instalación de Server Administrator* disponible en `dell.com/openmanagemanuals`.

Inicio de sesión único

La opción Inicio de sesión único en los sistemas operativos Windows permite que todos los usuarios que hayan iniciado sesión puedan omitir la página de inicio de sesión y puedan acceder a la aplicación web de Server Administrator al hacer clic en el icono **Server Administrator** del escritorio.

NOTA: Para obtener más información sobre el inicio de sesión único, consulte el artículo de la base de conocimientos en `support.microsoft.com/default.aspx?scid=kb;en-us;Q258063`.

Para acceder a la máquina local, deberá tener una cuenta en la máquina con los correspondientes privilegios (Usuario, Usuario avanzado o Administrador). El resto de usuarios deberán autenticarse en Microsoft Active Directory. Para iniciar Server Administrator utilizando la autenticación de inicio de sesión único de Microsoft Active Directory, también se deben aplicar los siguientes parámetros:

```
authType=ntlm&application=[plugin name]
```

donde `plugin name = omsa, ita,` , etc.

Por ejemplo,

```
https://localhost:1311/?authType=ntlm&application=omsa
```

Para iniciar Server Administrator utilizando la autentificación de inicio de sesión único con las cuentas de usuario de la máquina local, también se deben aplicar los siguientes parámetros:

```
authType=ntlm&application=[plugin name]&locallogin=true
```

Donde `plugin name = omsa, ita`, etc.

Por ejemplo,

```
https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true
```

Server Administrator también se ha ampliado para permitir que otros productos (como Dell EMC OpenManage Essentials) tengan acceso directo a las páginas web de Server Administrator sin pasar por la página de inicio de sesión (si está conectado actualmente y tiene los privilegios de usuario apropiados).

Configuración de seguridad en sistemas que ejecutan un sistema operativo Microsoft Windows compatible

Debe configurar los valores de seguridad del explorador para iniciar sesión en Server Administrator desde un sistema de administración remota que esté ejecutando un sistema operativo Microsoft Windows compatible.

Es posible que la configuración de seguridad del explorador impida la ejecución de las secuencias de comandos del lado cliente que Server Administrator utiliza. Para activar el uso de las secuencias de comandos del lado cliente, realice los pasos a continuación en el sistema de administración remota.

NOTA: Si no ha configurado el explorador para activar el uso de secuencias de comandos del lado cliente, es posible que vea una pantalla vacía al iniciar sesión en Server Administrator. En este caso, se mostrará un mensaje de error con instrucciones sobre cómo configurar los valores del explorador.

Activación del uso de secuencias de comandos en el lado del cliente en Internet Explorer

1. En el explorador web, haga clic en **Herramientas** > **Opciones de Internet** > **Seguridad.**
   Se muestra la ventana **Opciones de Internet**.
2. En **Seleccione una zona para ver o cambiar la configuración de seguridad**, haga clic en **Sitios de confianza y**, a continuación, haga clic en **Sitios**.
3. En el campo **Agregar este sitio web a la zona**, pegue la dirección web utilizada para acceder al sistema administrado remoto.
4. Haga clic en **Agregar**.
5. Copie la dirección web usada para acceder al sistema administrado remotamente desde la barra de dirección del explorador y péguela en el campo **Agregar este sitio web a la zona**.
6. En **Nivel de seguridad para esta zona,** haga clic en el nivel **Personalizado**.
7. Haga clic en **Aceptar** para guardar la nueva configuración.
8. Cierre el explorador e inicie sesión en Server Administrator.

Activación del inicio de sesión único de Server Administrator en Internet Explorer

Para permitir el inicio de sesión único de Server Administrator sin recibir avisos sobre credenciales de usuario:

1. En el explorador web, haga clic en **Herramientas** > **Opciones de Internet** > **Seguridad**
2. En **Seleccione una zona para ver o cambiar la configuración de seguridad**, haga clic en **Sitios de confianza y**, a continuación, haga clic en **Sitios**.
3. En el campo **Agregar este sitio web a la zona**, pegue la dirección web utilizada para acceder al sistema administrado remoto.
4. Haga clic en **Agregar**.
5. Haga clic en **Nivel personalizado**.
6. En **Autenticación de usuario**, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.
7. Haga clic en **Aceptar** para guardar la nueva configuración.
8. Cierre el explorador e inicie sesión en Server Administrator.

Activación del uso de secuencias de comandos en el lado del cliente en Mozilla Firefox

1. Abra el explorador.
2. Haga clic en **Editar** > **Preferencias**.
3. Seleccione **Avanzada** > **Secuencias de comandos y complementos**.
4. En Activar Javascript para, asegúrese de que la opción de navegador esté seleccionada. Asegúrese de que la casilla **Navegador** esté seleccionada en **Activar JavaScript para**.
5. Haga clic en **Aceptar** para guardar la nueva configuración.
6. Cierre el explorador.
7. Inicie sesión en Server Administrator.

Página de inicio de Server Administrator

NOTA: No utilice los botones de la barra de herramientas del explorador web (como **Atrás** y **Actualizar**) mientras utiliza Server Administrator. Use solamente las herramientas de navegación de Server Administrator.

Salvo algunas excepciones, la página de inicio de Server Administrator tiene tres áreas principales:

- La barra de navegación global proporciona vínculos a servicios generales.
- El árbol del sistema muestra todos los objetos visibles del sistema según los privilegios de acceso del usuario.
- La ventana de acciones muestra las acciones de administración disponibles para el objeto del árbol de sistema seleccionado según los privilegios de acceso del usuario. La ventana de acciones contiene tres áreas funcionales:

- Las fichas de acción muestran las acciones o categorías de acciones principales que están disponibles para el objeto seleccionado, según los privilegios de acceso del usuario.
- Las fichas de acción se dividen en subcategorías de todas las opciones secundarias disponibles para las fichas de acción, según los privilegios de acceso del usuario.
- El área de datos muestra información del objeto del árbol del sistema seleccionado, una ficha de acción y una subcategoría según los privilegios de acceso del usuario.

Asimismo, una vez conectado a la página de inicio de **Server Administrator**, en la esquina superior derecha de la ventana aparece el modelo del sistema, el nombre asignado del sistema y el nombre y los privilegios de usuario del usuario actual.

La siguiente tabla enumera los nombres de campo de la **interfaz gráfica de usuario** y el sistema aplicable, cuando se instala Server Administrator en el sistema.

Tabla 7. Nombres de campo de la interfaz gráfica de usuario y sistemas aplicables

Nombre de campo de la interfaz gráfica de usuario	Sistema al que se aplica
Gabinete modular	Sistema modular
Server Module	Sistema modular
Sistema principal	Sistema modular
Sistema	Sistema no modular
Chasis del sistema principal	Sistema no modular

La siguiente ilustración muestra un ejemplo de la página de inicio de Server Administrator para un usuario conectado con privilegios de administrador en un sistema no modular.

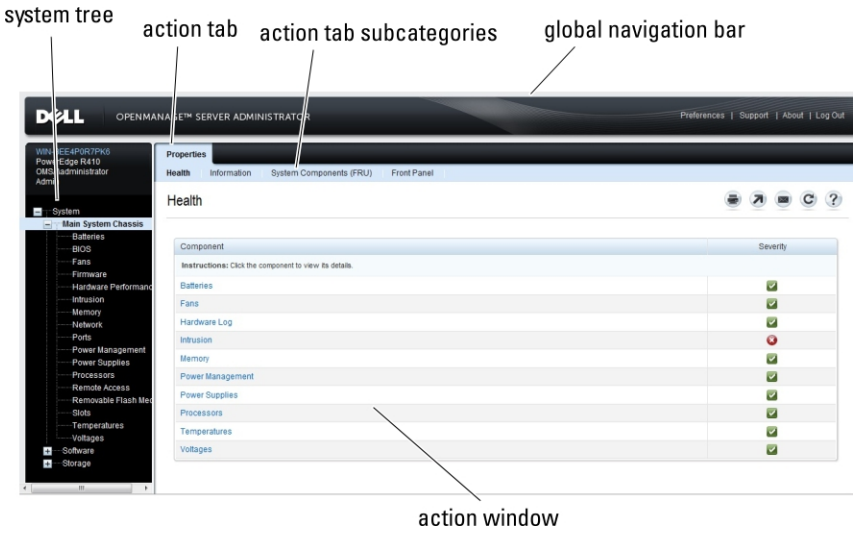

Ilustración 1. Ejemplo de la página de inicio de Server Administrator: sistema no modular

La siguiente ilustración muestra un ejemplo de la página de inicio de Server Administrator para un usuario conectado con privilegios de administrador en un sistema modular.

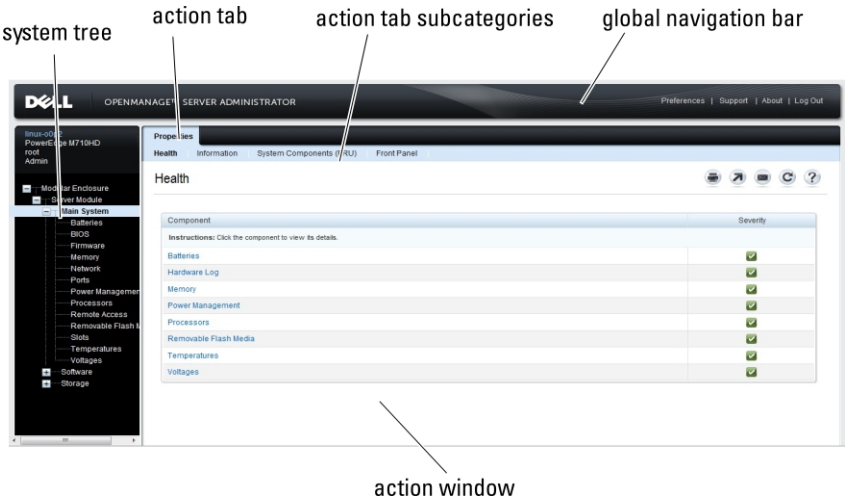

Ilustración 2. Ejemplo de la página de inicio de Server Administrator: sistema modular

Cuando se hace clic en un objeto del árbol del sistema se abre la ventana de acciones correspondiente a ese objeto. Puede navegar por la ventana de acciones a través de las fichas de acción para seleccionar categorías principales y a través de las subcategorías de la ficha de acción para acceder a información más detallada o acciones más específicas. La información que se muestra en el área de datos de la ventana de acciones puede incluir desde registros del sistema hasta indicadores de estado y medidas de sonda del sistema. Los elementos subrayados en el área de datos de la ventana de acciones indican un nivel más de funcionalidad. Cuando hace clic en un elemento subrayado se crea un área de datos en la ventana de acciones que contiene un mayor nivel de detalle. Por ejemplo, cuando se hace clic en **Chasis del sistema principal/Sistema principal** en la subcategoría **Estado** de la ficha de acción **Propiedades** se muestra el estado de todos los componentes contenidos en el objeto Chasis del sistema principal/Sistema principal que se supervisan para comprobar el estado.

NOTA: Se necesitan privilegios de administrador o usuario avanzado para ver muchos de los objetos del árbol de sistema, los componentes del sistema, las fichas de acción y las funciones del área de datos que pueden configurarse. Además, únicamente los usuarios que hayan iniciado sesión con privilegios de administrador pueden acceder a funciones esenciales del sistema, como la funcionalidad de apagado, incluida en la ficha **Apagado**.

Diferencias de la interfaz de usuario de Server Administrator entre sistemas modulares y no modulares

En la siguiente tabla se enumeran las funciones de Server Administrator disponibles en sistemas modulares y no modulares.

Tabla 8. Diferencias de la interfaz de usuario de Server Administrator en sistemas modulares y no modulares

Características	Sistema modular	Sistema no modular
Baterías	✓	✓
Fuentes de alimentación	✗	✓
Ventiladores	✗	✓
Rendimiento del hardware	✗	✓
Intrusión	✗	✓
Memoria	✓	✓
Red	✓	✓

Tabla 8. Diferencias de la interfaz de usuario de Server Administrator en sistemas modulares y no modulares

Características	Sistema modular	Sistema no modular
Puertos	✓	✓
Administración de energía	✓	✓
Procesadores	✓	✓
Acceso remoto	✓	✓
Medios flash extraíbles	✓	✓
Ranuras	✓	✓
Temperaturas	✓	✓
Voltajes	✓	✓
Gabinete modular (información del chasis y de CMC)	✓	✗

Barra de navegación global

La barra de navegación global y sus vínculos están disponibles para todos los niveles de usuario del programa.

- Haga clic en **Preferencias** para abrir la página de inicio **Preferencias**. Consulte Uso de la página de inicio de preferencias.
- Haga clic en **Asistencia** para conectarse al sitio web de asistencia de Dell EMC.
- Haga clic en **Acerca de** para mostrar información de copyright y la versión de Server Administrator.
- Haga clic en **Cerrar sesión** para finalizar la actual sesión del programa de Server Administrator.

Árbol del sistema

El árbol del sistema aparece en el lado izquierdo de la página de inicio de Server Administrator y enumera los componentes del sistema que se pueden mostrar. Los componentes del sistema se clasifican por tipo de componente. Cuando expande el objeto principal conocido como **Gabinete modular** > **Módulo del servidor/sistema**, las categorías principales de componentes del módulo del servidor/sistema que pueden aparecer son **Chasis del sistema principal/Sistema principal**, **Software**y **Almacenamiento**.

Para expandir una rama del árbol, haga clic en el signo más (⊞) que se encuentra a la izquierda de un objeto o haga doble clic en el objeto. El signo menos (⊟) indica una entrada expandida que no se puede seguir expandiendo.

Ventana de acciones

Cuando hace clic en un elemento del árbol del sistema, aparecen detalles sobre el componente o el objeto en el área de datos de la ventana de acciones. Si hace clic en una ficha de acción, se muestran todas las opciones disponibles para el usuario en una lista de subcategorías.

Si hace clic en un objeto del árbol del módulo del servidor/sistema, se abre la ventana de acciones de ese componente y se muestran las fichas de acción disponibles. En el área de datos, aparece de forma predeterminada una subcategoría preseleccionada de la primera ficha de acción del objeto seleccionado.

Por lo general, la subcategoría preseleccionada es la primera opción. Por ejemplo, si hace clic en el objeto **Chasis del sistema principal/ Sistema principal**, se abre una ventana de acciones en la que se muestran la ficha de acción **Propiedades** y la subcategoría **Estado** en el área de datos de la pestaña.

Área de datos

El área de datos se ubica debajo de las fichas de acción en el lado derecho de la página de inicio. El área de datos es donde se realizan las tareas o se ven los detalles sobre los componentes del sistema. El contenido de la ventana depende del objeto del árbol del sistema y de la ficha de acción seleccionada en ese momento. Por ejemplo, cuando elige **BIOS** en el árbol del sistema, selecciona de forma predeterminada la ficha **Propiedades** y la información de la versión del BIOS del sistema aparece en el área de datos. El área de datos de la ventana de acciones contiene muchas funciones comunes, incluidos los indicadores de estado, los botones de tareas, los elementos subrayados y los indicadores de medida.

La interfaz de usuario de Server Administrator muestra la fecha en formato <mm/dd/aaaa>.

Indicadores de estado de los componentes del módulo del servidor o sistema

Los iconos que aparecen junto a los nombres de los componentes muestran el estado de esos componentes (desde la última actualización de la página).

Tabla 9. Indicadores de estado de los componentes del módulo del servidor o sistema

Descripción	Icono
	El componente se encuentra en condición satisfactoria (normal).
	El componente presenta una condición de aviso (no crítica). Una condición de aviso se produce cuando una sonda u otra herramienta de supervisión detecta una lectura de un componente que está dentro de determinados valores mínimos y máximos. Una condición de aviso requiere una pronta atención.
	El componente presenta una condición crítica o de error. Una condición crítica se produce cuando una sonda u otra herramienta de supervisión detecta una lectura de un componente que está dentro de determinados valores mínimos y máximos. Una condición crítica requiere atención inmediata.
	No se conoce la condición del componente.

Botones de tareas

La mayoría de las ventanas que se abren desde la página de inicio de Server Administrator contienen al menos cinco botones de tareas: **Imprimir**, **Exportar**, **Correo electrónico**, **Ayuda** y **Actualizar**. Existen otros botones de tareas incluidos en las ventanas específicas de Server Administrator. Por ejemplo, la ventana **Registro** también contiene los botones de tareas **Guardar como** y **Borrar registro**.

- Cuando hace clic en **Imprimir** ( ), se imprime una copia de la ventana abierta en la impresora predeterminada.
- Cuando hace clic en **Exportar** ( ), se genera un archivo de texto que enumera los valores de cada campo de datos en la ventana abierta. El archivo de exportación se guardará en la ubicación que especifique. Para obtener más información sobre cómo personalizar el delimitador que separa los valores de los campos de datos, consulte Configuración de las preferencias del usuario y del sistema.
- Cuando hace clic en **Correo electrónico** ( ), se crea un mensaje de correo electrónico dirigido al destinatario de correo electrónico designado. Para obtener instrucciones sobre cómo configurar el servidor de correo electrónico y destinatario predeterminado de correo electrónico, consulte Configuración de las preferencias del usuario y del sistema.
- Cuando hace clic en **Actualizar** ( ), se vuelve a cargar la información de estado del componente del sistema en el área de datos de la ventana de acciones.
- Al hacer clic en **Guardar como**, se guarda un archivo HTML de la ventana de acciones en un archivo **.zip**.
- Al hacer clic en **Borrar registro**, se borran todos los eventos del registro mostrados en el área de datos de la ventana de acciones.
- Cuando hace clic en **Ayuda** ( ), se proporciona información detallada sobre una ventana específica o el botón de tareas que esté viendo.

NOTA: Los botones **Exportar**, **Correo electrónico** y **Guardar como** son visibles solo para los usuarios conectados con privilegios de usuario avanzado o administrador. El botón **Borrar registro** es visible solo para usuarios con privilegios de administrador.

Elementos subrayados

Cuando hace clic en un elemento subrayado del área de datos de la ventana de acciones, se muestran detalles adicionales de ese elemento.

Indicadores de medida

El indicador de medida representa las sondas de temperatura, las sondas del ventilador y las sondas de voltaje. Por ejemplo, la siguiente figura muestra la lectura de la sonda del ventilador de CPU de un sistema.

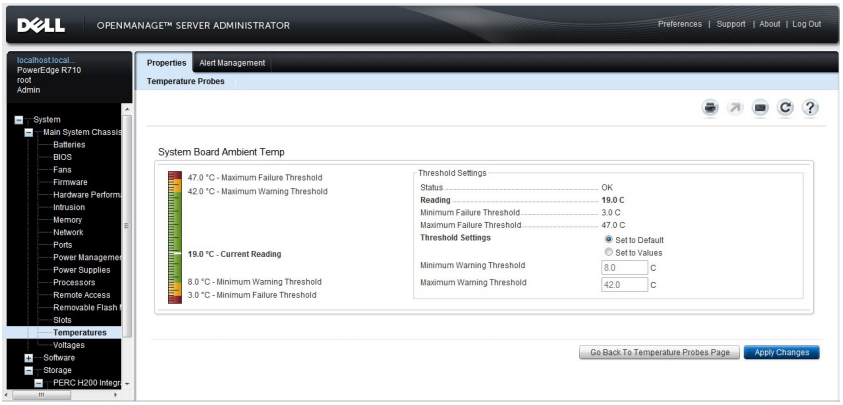

Ilustración 3. Indicador de medida

Uso de la ayuda en línea

La ayuda contextual en línea está disponible para todas las ventanas de la página de inicio de Server Administrator. Al hacer clic en **Ayuda**, se abre una ventana de ayuda independiente que contiene información detallada sobre la ventana específica que está viendo. La ayuda en línea está diseñada para orientarlo a través de acciones específicas necesarias para implementar todos los aspectos de los servicios de Server Administrator. La ayuda en línea está disponible para todas las ventanas que se pueden ver, según los grupos de software y hardware que Server Administrator descubra en el sistema y según el nivel de privilegio del usuario.

Uso de la página de inicio de preferencias

El panel izquierdo de la página de inicio de preferencias (donde se muestra el árbol del sistema en la página de inicio de Server Administrator) muestra todas las opciones de configuración disponibles en la ventana del árbol del sistema.

Las opciones de configuración disponibles de la página de inicio Preferencias son las siguientes:

- Configuración general
- Administrador del servidor

Puede ver la ficha **Preferencias** después de iniciar sesión para administrar un sistema remoto. Esta ficha también está disponible cuando inicia sesión para administrar Server Administrator Web Server o el sistema local.

Al igual que la página de inicio de Server Administrator, la página de inicio **Preferencias** contiene tres áreas principales:

- La barra de navegación global proporciona vínculos a servicios generales.
  - Haga clic en **Inicio** para volver a la página de inicio de Server Administrator.
- El panel izquierdo de la página de inicio **Preferencias** (donde se muestra el árbol del sistema en la página de inicio de Server Administrator) muestra las categorías de preferencia del sistema administrado o de Server Administrator Web Server.
- La ventana de acciones muestra los valores y las preferencias disponibles del sistema administrado o de Server Administrator Web Server.

Preferencias en el sistema administrado

Al iniciar sesión en un sistema remoto, de manera predeterminada la página de inicio de preferencias muestra la ventana **Configuración de nodo** bajo la ficha **Preferencias**.

Haga clic en el objeto Server Administrator para habilitar o deshabilitar el acceso de los usuarios con privilegios de usuario o usuario avanzado. En función de los privilegios del grupo del usuario, la ventana de acciones del objeto Server Administrator puede incluir la ficha **Preferencias**.

En la ficha **Preferencias** se puede:

- Activar o desactivar el acceso de usuarios con privilegios de usuario o de usuario avanzado.
- Seleccionar el formato de los mensajes de alerta.

  NOTA: Los formatos posibles son **tradicional** y **mejorado**. El formato predeterminado es **tradicional**, que es el formato heredado.
- Activa la copia de seguridad automática y Borrar entradas de registro de ES

  Esta función está deshabilitada de manera predeterminada. Habilitar esta función le permite crear una copia de seguridad automática de los registros ESM. Una vez creada la copia de seguridad, se borran los registros ESM de Server Administrator y las entradas de SEL del iDRAC/BMC. El proceso se repite siempre que los registros estén llenos.

  La copia de seguridad se guarda en:

  Windows: `<Install_root>\omsa\log\omsellog.xml`

  Linux y ESXi: `<Install_root>/var/log/openmanage/omsellog.xml`

  NOTA: Esta característica solo está disponible en los servidores PowerEdge de 10.ª y 11.ª generación. El iDRAC ofrece funciones de eliminación automática de copia de seguridad y registro de SEL a partir de los servidores PowerEdge de 12.ª generación.
- Seleccione o borre las gravedades de las entradas de registro ingresadas en el registro de eventos principales de los sistemas operativos. Seleccione los valores posibles: **Registrar eventos críticos**, **Aviso de registro** o **Registro informativo**

  NOTA: De manera predeterminada, todas las opciones están seleccionadas. La función del filtro de registro del sistema operativo está disponible cuando el filtro de registro del sistema operativo está instalado.
- Seleccione **Habilitar** para registrar todos los sucesos de sensor ESM no supervisados. Si se habilita esta función, Server Administrator genera capturas de SNMP, registros del sistema operativo y alertas para todos los sensores no supervisados.
- Configurar el tamaño del registro de comandos.
- Configurar SNMP

Preferencias de Server Administrator Web Server

Cuando inicia sesión para administrar Server Administrator Web Server, de forma predeterminada la página de inicio Preferencias muestra la ventana Preferencias de usuario en la ficha **Preferencias**.

Debido a la separación entre Server Administrator Web Server y el sistema administrado, las siguientes opciones aparecen cuando inicia sesión en Server Administrator Web Server mediante el vínculo Administrar Web Server:

- Preferencias de Web Server
- Administración de certificado X.509

Para obtener más información acerca de cómo acceder a estas funciones, consulte Descripción general de los servicios de Server Administrator.

Servicio de conexión y configuración de seguridad de la administración de servidores de Systems Management

Configuración de las preferencias del usuario y del sistema

Puede establecer las preferencias del usuario y del servidor web en la página de inicio **Preferencias**.

NOTA: Debe estar conectado con privilegios de administrador para establecer o restablecer las preferencias del sistema o del usuario.

Para configurar las preferencias de usuario:

1. Haga clic en **Preferencias** en la barra de navegación global.

   Aparece la página de inicio **Preferencias**.
2. Haga clic en **Configuración general**.
3. Para agregar un destinatario de correo electrónico preseleccionado, escriba la dirección de correo electrónico del contacto del servicio designado en el campo **Destinatario:** y haga clic en **Aplicar**.

NOTA: Haga clic en **Correo electrónico** () en cualquier ventana para enviar un mensaje de correo electrónico con un archivo HTML adjunto de la ventana a la dirección de correo electrónico designada.

NOTA: La dirección URL de Web Server no se conserva si reinicia el servicio de Server Administrator o el sistema donde está instalado Server Administrator. Use el comando **omconfig** para volver a agregar la dirección URL.

Preferencias de Web Server.

Siga estos pasos para configurar las preferencias del usuario:

1. Haga clic en **Preferencias** en la barra de navegación global.

   Aparece la página de inicio **Preferencias**.
2. Haga clic en **Configuración general**.
3. En la ventana **Preferencias del servidor**, establezca las opciones conforme sea necesario.
   - La función **Tiempo de espera de la sesión (minutos)** se puede utilizar para establecer el límite de tiempo que permanece activa una sesión de Server Administrator. Seleccionar **Activar** le permite a Server Administrator agotar el tiempo de espera si no hay interacción del usuario durante un número especificado de minutos. Los usuarios a cuyas sesiones se les ha acabado el tiempo de espera deben iniciar sesión nuevamente para continuar. Seleccionar **Desactivar** desactiva la función de **Tiempo de espera de la sesión (minutos)** de Server Administrator.
   - El campo **Puerto HTTPS** especifica el puerto para Server Administrator. El puerto seguro predeterminado para Server Administrator es 1311.

     NOTA: Si se cambia el número de puerto a uno no válido o en uso, se puede impedir que otras aplicaciones o exploradores accedan a Server Administrator en el sistema administrado. Para ver la lista de puertos predeterminados, consulte la *Guía de instalación de Server Administrator* disponible en **dell.com/openmanagemanuals**.
   - El campo **Dirección IP a la cual enlazar** especifica las direcciones IP para el sistema administrado a las que se enlaza Server Administrator cuando se inicia una sesión. Seleccione **Todas** para enlazar con todas las direcciones IP aplicables para el sistema. Seleccione **Específica** para enlazar con una dirección IP específica.

     NOTA: Si se cambia el valor de **Dirección IP a la cual enlazar** a otro valor que no sea **Todas**, es posible que otras aplicaciones o exploradores no puedan acceder a Server Administrator en el sistema administrado.
   - El campo **Destinatario** especifica las direcciones de correo electrónico a las cuales desea enviar correos electrónicos acerca de actualizaciones de manera predeterminada. Puede configurar varias direcciones de correo electrónico y utilizar una coma para separar cada una de ellas.
   - Los campos **Nombre de Servidor SMTP (o Dirección IP)** y **Sufijo DNS para servidor SMTP** especifican el protocolo simple de transferencia de correo (SMTP) y el sufijo del Domain Name System (DNS) de la empresa u organización. Para que Server Administrator pueda enviar mensajes de correo electrónico, debe escribir la dirección IP y el sufijo DNS del servidor SMTP de la empresa u organización en los campos apropiados.

     NOTA: Por motivos de seguridad, es posible que la empresa u organización no permita que se envíen mensajes de correo electrónico a través del servidor SMTP a cuentas externas.
   - El campo **Tamaño de registro de comandos** especifica el tamaño del archivo más grande en MB para el archivo de registro de comandos.

     NOTA: Este campo solo aparece al iniciar sesión para administrar Server Administrator Web Server.
   - El campo **Vínculo de asistencia** especifica la dirección URL de la entidad empresarial que proporciona asistencia al sistema administrado.
   - El campo **Delimitador personalizado** especifica el carácter que se utiliza para separar los campos de datos creados con el botón **Exportar**. El carácter **;** es el delimitador predeterminado. Otras opciones son **!**, **@**, **#**, **$**, **%**, **^**, *, **~**, **?**, **|**, y **,**.
   - El campo **Cifrado SSL** especifica una conexión segura entre el servidor web y el explorador. Elija los cifrados que admitan el servidor web al configurar. El servicio de conexión no se inicia si se establece un conjunto de cifrados no válido. De manera predeterminada, los siguientes son los valores de conjunto de cifrado:

     `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`

     `,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,`

     `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`

     `TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,`

     `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,`

     `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`

`TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,`

`TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,`

`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,`

`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,`

`TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,`

`TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA`

NOTA: Si se establece un valor de cifrado incorrecto y si el servicio de conexión no se inicia, utilice la solicitud del comando CLI o establezca manualmente los cifrados válidos y vuelva a iniciar el servicio de conexión.

NOTA: La actualización a Server Administrator 9.1 no conservará la configuración de cifrado del servidor web existente por razones de seguridad.

- El campo **Protocolos SSL** le permite la configuración desde los protocolos SSL enumerados en el servidor web para establecer una conexión HTTPS. Los valores posibles son: `TLSv1.1,` , y `TLSv1.2 (TLSv1.1, TLSv1.2)`. De manera predeterminada, el valor del protocolo SSL se establece en `(TLSv1.1, TLSv1.2)`. Los cambios surten efecto después de que se reinicia el servidor web.

  NOTA: Si el protocolo no es compatible con las configuraciones predeterminadas, active el protocolo SSL desde la configuración del explorador.
- **Algoritmo de firma clave (para certificado autoconfirmado)**: le permite seleccionar un algoritmo de firma admitido. Si selecciona **SHA 512** o **SHA 256**, asegúrese de que el explorador o el sistema operativo admitan este algoritmo. Si selecciona una de estas opciones sin contar con un explorador o sistema operativo compatible, Server Administrator mostrará el error `cannot display the webpage`. Este campo está disponible solo para los certificados firmados y generados automáticamente de Server Administrator. La lista desplegable se atenuará si importa o genera certificados nuevos en Server Administrator.
- **Java Runtime Environment**: permite seleccionar una de las siguientes opciones:
  - **JRE enlazado**: permite el uso de JRE suministrado con el administrador del sistema.
  - **JRE del sistema**: permite el uso de la instancia de JRE instalada en el sistema. Seleccione la versión requerida en la lista desplegable.

    NOTA: Server Administrator no recomienda la actualización a versiones principales de Java Runtime Environment (JRE), se limita a parches de seguridad y versiones menores. Para obtener más información, consulte las notas de la versión de Server Administrator (incluidas en la aplicación de Server Administrator) o visite `dell.com/openmanagemanuals`.

    NOTA: Si JRE no existe en el sistema donde se ejecuta Server Administrator, se utiliza la instancia de JRE suministrada con Server Administrator.

4. Cuando haya terminado de configurar las opciones en la ventana **Preferencias del servidor**, haga clic en **Aplicar**.

   NOTA: Reinicie Server Administrator Web Server para que los cambios se apliquen.

Administración de certificado X.509

NOTA: Para realizar la administración de certificados debe estar conectado con privilegios de administrador.

Los certificados web son necesarios para asegurar la identidad de un sistema remoto y garantizan que nadie pueda ver ni cambiar la información que se intercambia con el sistema remoto. Para asegurar la seguridad del sistema, se recomienda que:

- Genere un nuevo certificado X.509, utilice nuevamente un certificado X.509 existente o importe una cadena de certificados de una entidad de certificación (CA).
- Todos los sistemas con Server Administrator instalado cuentan con nombres únicos de host.

Para administrar certificados X.509 mediante la página de inicio **Preferencias**, haga clic en **Configuración general**, después en la ficha **Web Server** y finalmente en **Certificado X.509**.

A continuación, se indican las opciones disponibles:

- **Generar un certificado nuevo**: Genera un certificado autofirmado nuevo que se usa para que SSL se comunique con el servidor que ejecuta Server Administrator y el explorador.

  NOTA: Cuando se usa un certificado autofirmado, la mayoría de los exploradores web muestran una advertencia de *sin confianza* ya que el certificado autofirmado no está firmado por una Autoridad de certificados (AC) de confianza para el sistema operativo.

Algunas configuraciones de seguridad de los exploradores también pueden bloquear los certificados SSL autofirmados. La GUI web de Server Administrator necesita un certificado firmado por una AC para dichos exploradores seguros.

- **Mantenimiento de certificados:** le permite generar una solicitud de firma de certificado (CSR) que contiene toda la información del certificado acerca del host para que la CA automatice la creación de un certificado web SSL de confianza. Puede recuperar el archivo CSR necesario desde las instrucciones en la página de solicitud de firma de certificado (CSR), o bien puede copiar el texto entero en el cuadro de texto en la página de solicitud de firma de certificado y pegarlo en el formulario de envío para la CA. El texto debe estar en el formato codificado Base64.

  NOTA: Además tiene la opción de ver la información del certificado y exportar el certificado que se esté usando al formato codificado Base64, que se puede importar a través de otros servicios web.
- **Importar una cadena de certificados**: le permite importar la cadena de certificados (en formato PKCS # 7) firmados por una autoridad de certificados reconocida. El certificado puede estar en formato DER o en formato codificado Base64.
- **Importar un almacén de claves de PKCS12**: permite importar una almacén de claves PKCS # 12 que reemplaza la clave privada y el certificado utilizados en el servidor web de Server Administrator. PKCS # 12 es un almacén de claves público que contiene una clave privada y el certificado para un servidor web. Server Administrator utiliza el formato clasificación de claves Java (JKS) para almacenar los certificados SSL y su clave privada. La importación de un almacén de claves PKCS # 12 en Server Administrator elimina las anotaciones de clasificación de claves e importa las anotaciones de clave privada y certificado a la JKS de Server Administrator.

  NOTA: Aparece un mensaje de error si se selecciona un archivo PKCS no válido o si se escribe una contraseña incorrecta.

Certificados de servidor SSL

Server Administrator Web Server está configurado para usar el protocolo de seguridad SSL estándar del sector para transferir datos cifrados a través de una red. Basado en una tecnología de cifrado asimétrico, el SSL está ampliamente aceptado para facilitar una comunicación autenticada y cifrada entre clientes y servidores a fin de evitar manipulaciones en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Autentificarse ante un cliente habilitado con SSL
- Permitir a los dos sistemas establecer una conexión cifrada

El proceso de cifrado proporciona un alto nivel de protección de datos. Server Administrator utiliza la forma de cifrado más segura, disponible habitualmente para los exploradores de Internet en Norteamérica.

Server Administrator Web Server cuenta con un certificado digital SSL exclusivo autofirmado de manera predeterminada. Puede reemplazar el certificado SSL predeterminado por un certificado firmado por una Autoridad de certificados (CA) conocida. Una Autoridad de certificados es una entidad comercial reconocida en la industria de TI por cumplir con altas normas de filtrado confiable, identificación y otro criterios de seguridad importantes. Algunas Autoridades de certificados son Thawte y VeriSign. Para iniciar el proceso de obtención de un certificado firmado por una CA, utilice la interfaz web de Server Administrator para generar una solicitud de firma de certificado (CSR) con la información de su empresa. A continuación, envíe la CSR generada a una CA como VeriSign o Thawte. La CA puede ser una CA raíz o una CA intermedia. Una vez que reciba el certificado SSL firmado por una CA, cargue el certificado en Server Administrator.

Para que la estación de administración considere a cada Server Administrator un elemento de confianza, es necesario incluir el certificado SSL de dicho Server Administrator en el almacén de certificados de la estación de administración. Una vez instalado el certificado SSL en las estaciones de administración, los exploradores admitidos pueden acceder a Server Administrator sin avisos de certificados.

Fichas de acción de Server Administrator Web Server

A continuación, se indican las fichas de acción que aparecen cuando se inicia sesión para administrar Server Administrator Web Server:

- Propiedades
- Apagado
- Registros
- Administración de alertas
- Administración de sesiones

Actualización de Web Server

PRECAUCIÓN: El restablecimiento a los valores de fábrica no es posible después de una actualización de Web Server. Para restablecer los valores de fábrica, vuelva a instalar Server Administrator.

Puede actualizar el servidor web de Apache Tomcat cuando sea necesario mediante **omwsupdateutility** sin afectar la funcionalidad de Server Administrator. La utilidad permite actualizar a una versión inferior del servidor web pero no admite la actualización a una versión

superior. Por ejemplo, se admite la actualización desde la versión A.*x* a A.*y* pero no de A.*x* a B.*x* o B.*y*. Además, el uso de la utilidad puede mover la versión del servidor web a una versión anterior, siempre que sea inferior. La utilidad se guarda en la siguiente ubicación predeterminada durante la instalación del servidor de web:

- En sistemas que ejecutan el sistema operativo Windows: `C:\Program Files\Dell\SysMgt\omsa\wsupdate`
- En sistemas que ejecutan el sistema operativo Linux: `/opt/dell/srvadmin/lib64/openmanage/wsupdate`

Puede descargar la versión requerida del paquete de servidor web Tomcat y ejecutar la utilidad desde una solicitud de comando. Descargue el paquete de distribución principal del servidor web Tomcat desde `tomcat.apache.org`. El paquete de distribución debe ser un archivo.zip o.tar.gz. No se admiten paquetes de instalación de Windows.

Para actualizar el servidor web, navegue hasta la carpeta **wsupdate** y, a continuación, ejecute el siguiente comando:

- En Windows: `omwsupdate.bat [SysMgt folder path] [apache-tomcat.zip/.tar.gz file path]`
- En Linux: `omwsupdate.sh [srvadmin folder path] [apache-tomcat.zip/.tar.gz file path]`

La ruta de acceso de la carpeta predeterminada **SysMgt** es `C:\Program Files\Dell\SysMgt` y la ruta de acceso de la carpeta **srvadmin** es `/opt/dell/srvadmin`.

Uso de la interfaz de línea de comandos de Server Administrator

La interfaz de línea de comandos (CLI) de Server Administrator permite a los usuarios realizar tareas esenciales de administración de sistemas desde el símbolo de sistema del sistema operativo de un equipo supervisado.

La CLI permite que un usuario que tenga una tarea muy bien definida pueda recuperar rápidamente información acerca del sistema. Por ejemplo, mediante el uso de los comandos de CLI, los administradores pueden escribir programas o secuencias de comandos por lotes para ejecutarlos en momentos específicos. Cuando estos programas se ejecutan, pueden capturar informes sobre componentes de interés, como las rpm de un ventilador. Con secuencias de comandos adicionales, la CLI se puede usar para capturar datos durante períodos de mucho uso del sistema para realizar una comparación con las mismas mediciones en los momentos de poco uso del sistema. Los resultados de los comandos se pueden enrutar a un archivo para su posterior análisis. Los informes pueden ayudar a los administradores a obtener información que se puede usar para ajustar los patrones de uso, a fin de justificar la compra de nuevos recursos de sistema o para enfocarse en la condición de un componente con problemas.

Para obtener instrucciones completas sobre la funcionalidad y el uso de la CLI, consulte la *Guía de la interfaz de línea de comandos de Server Administrator* en `dell.com/openmanagemanuals`.

4

Servicios de Server Administrator

Server Administrator Instrumentation Service supervisa la condición de un sistema y proporciona acceso rápido a la información detallada sobre los errores y el rendimiento mediante agentes de administración de sistemas estándar del sector. Las funciones de informes y visualización permiten la recuperación del estado general de la condición para cada chasis que integra el sistema. En el nivel de subsistema, puede ver información acerca de voltajes, temperaturas, rpm de ventiladores y funciones de la memoria en puntos clave del sistema. En la vista de resumen es posible ver una cuenta detallada de cada costo de propiedad (COO) relevante del sistema. También se puede recuperar la información de la versión para el BIOS, firmware, sistema operativo y todo el software de administración de los sistemas instalados.

Asimismo, los administradores de sistemas pueden utilizar Instrumentation Service para realizar las siguientes tareas esenciales:

- Especificar los valores máximos y mínimos para ciertos componentes esenciales. Los valores, denominados umbrales, determinan el rango en el cual se produce un evento de aviso para ese componente (los valores de error mínimos y máximos los especifica el fabricante del sistema).
- Especificar cómo responde el sistema cuando ocurre un evento de aviso o error. Los usuarios pueden configurar las acciones que lleva a cabo un sistema en respuesta a las notificaciones de eventos de aviso y error. De manera alternativa, los usuarios que cuentan con una supervisión continua pueden especificar que no se lleve a cabo ninguna acción y valerse del juicio humano para seleccionar la mejor acción en respuesta a un evento.
- Completar todos los valores que pueden ser especificados por el usuario para el sistema, como el nombre del sistema, el número telefónico del usuario principal del sistema, el método de depreciación y si el sistema es arrendado o propio.

NOTA: Para obtener más información acerca de cómo configurar SNMP, consulte Configuración del agente SNMP en sistemas que ejecutan sistemas operativos Windows admitidos.

Temas:

Administración del sistema

La página principal de Server Administrator pasa al objeto Sistema de la vista de árbol de sistema. De manera predeterminada, se abren los componentes **Estado** en la ficha **Propiedades** para el objeto**Sistema**.

De forma predeterminada, la página de inicio **Preferencias** abre la opción **Configuración de nodos**.

En la página de inicio **Preferencias** es posible restringir el acceso de usuarios con privilegios de usuario y usuario avanzado, establecer la contraseña de SNMP y configurar los valores de usuario y del servicio de conexión SM SA.

NOTA: La ayuda contextual en línea está disponible para todas las ventanas de la página de inicio de Server Administrator. Haga clic en **Ayuda** ( ) para abrir una ventana de ayuda independiente que contiene información detallada sobre la ventana específica que está viendo. La ayuda en línea está diseñada para orientarlo a través de acciones específicas necesarias para implementar todos los aspectos de los servicios de Server Administrator. La ayuda en línea está disponible para todas las ventanas que se pueden ver, según los grupos de software y hardware que Server Administrator descubra en el sistema y según el nivel de privilegio del usuario.

NOTA: Debe contar con privilegios de administrador o usuario avanzado para ver muchos de los objetos del árbol del sistema, los componentes del sistema, las fichas de acción y las funciones del área de datos que se pueden configurar. Además, únicamente los usuarios que hayan iniciado sesión con privilegios de administrador pueden acceder a funciones esenciales del sistema, como la funcionalidad de apagado, incluida en la ficha **Apagado**.

Administración de objetos del árbol del módulo del servidor o sistema

El sistema de Server Administrator o árbol del módulo del servidor muestra todos los objetos del sistema visibles según los grupos de software y hardware que Server Administrator descubre en el sistema administrado y en los privilegios de acceso del usuario. Los componentes del sistema se clasifican por tipo de componente. Cuando expande el objeto principal: **Gabinete modular**: **Módulo del servidor/sistema**: las categorías principales de componentes del sistema que pueden aparecer son: **Chasis del sistema principal/ Sistema principal**, **Software**, y **Almacenamiento**.

Si Storage Management Service está instalado, según la controladora y el almacenamiento conectados al sistema, el objeto del árbol Almacenamiento se expande para mostrar varios objetos.

Para obtener información detallada sobre el componente Storage Management Service, consulte la *Guía del usuario de Storage Management* en **dell.com/openmanagemanuals**.

Objetos del árbol del sistema de la página de inicio de Server Administrator

Esta sección ofrece información acerca de los objetos del árbol del sistema en la página de inicio de Server Administrator. Debido a las limitaciones de los sistemas operativos ESXi, algunas características que se encuentran disponibles en versiones anteriores de Server Administrator no se encuentran disponibles en esta versión.

Las funcionalidades no admitidas por ESXi son:

- Información acerca de la compatibilidad FCoE y la compatibilidad iSoE
- Administración de alertas: acciones de alerta
- Interfaz de red: estado administrativo, DMA, dirección de protocolo de Internet (IP)
- Interfaz de red: estado operativo
- Apagado remoto: ciclo de encendido del sistema con apagado de sistema operativo primero
- Acerca de los detalles: detalles del componente Server Administrator especificados en la ficha **Detalles**
- Mapa de funciones

NOTA: Server Administrator siempre muestra la fecha en formato *<mm/dd/aaaa>*.

NOTA: Se necesitan privilegios de administrador o usuario avanzado para ver muchos de los objetos del árbol de sistema, componentes del sistema, fichas de acción y funciones del área de datos que pueden configurarse. Además, únicamente los usuarios que hayan iniciado sesión con privilegios de administrador pueden acceder a funciones esenciales del sistema, como la funcionalidad de apagado incluida en la ficha **Apagado**.

Gabinete modular

NOTA: A los efectos de Server Administrator, gabinete modular hace referencia a un sistema que puede contener uno o más sistemas modulares que se muestran como un módulo de servidor separado en el árbol del sistema. Al igual que un módulo de servidor independiente, un gabinete modular contiene todos los componentes esenciales de un sistema. La única diferencia es que existen ranuras para al menos dos módulos de servidor dentro de un contenedor más grande y cada uno de ellos es un sistema igual de completo que un módulo de servidor.

Para ver la información del chasis del sistema modular y la información de Chassis Management Controller (CMC), haga clic en el objeto **Gabinete modular**.

- **Ficha: Propiedades**
- **Subficha: Información**

En la ficha Propiedades, se puede:

- Ver la información de chasis del sistema modular que se supervisa.
- Ver la información detallada de Chassis Management Controller (CMC) del sistema modular que se supervisa.

Acceso y uso de Chassis Management Controller

Para iniciar la ventana **Inicio de sesión** de Chassis Management Controller desde la página de inicio de Server Administrator:

1. Haga clic en el objeto **Gabinete modular**
2. Haga clic en la ficha **Información de CMC** y, a continuación, haga clic en **Iniciar la interfaz web del CMC**. La ventana **Inicio de sesión** de CMC aparecerá.

Después de conectarse con CMC podrá supervisar y administrar el gabinete modular.

Propiedades del módulo del servidor o sistema

El objeto **Módulo del servidor o sistema** contiene tres grupos principales de componentes de sistema: Chasis del sistema principal/ Sistema principal, Softwarey Almacenamiento. La página principal de Server Administrator pasa al objeto **Sistema** de la vista de árbol de sistema. La mayoría de las funciones administrativas se pueden administrar desde la ventana de acciones del objeto **Módulo del servidor/ sistema**. La ventana de acciones del objeto **Módulo del servidor/sistema** tiene las siguientes fichas, en función de los privilegios del grupo del usuario: **Concesión de licencias**, **Propiedades**, **Apagado**, **Registros**, **Administración de alertas** y **Administración de sesiones**

Licencias

Subfichas: Información | Licencias

En la subficha Licencias, se puede:

- Configurar las preferencias para usar Integrated Dell Remote Access Controller (iDRAC) a fin de importar, exportar, eliminar o reemplazar la licencia digital de hardware.
- Ver los detalles del dispositivo usado. Los detalles incluyen el estado de la licencia, la descripción de la licencia, la id. de autorización y la fecha de vencimiento de la licencia.

  NOTA: Server Administrator admite la función de concesión de licencias a partir de los sistemas PowerEdge de 12.ª generación. Esta función está disponible solo si la versión mínima requerida de iDRAC (1.30.30) está instalada.

  NOTA: La función está disponible solo si la versión mínima requerida de iDRAC está instalada.

Propiedades

Subfichas: Condición | Resumen | Información de propiedad | Recuperación automática

En la ficha **Propiedades**, se puede:

- Ver el estado de alerta de la condición actual de los componentes de hardware y software en el objeto **Chasis del sistema principal/ Sistema principal** y el objeto **Almacenamiento**.
- Ver información de resumen detallada de todos los componentes del sistema que se supervisa.
- Ver y configurar la información de propiedad del sistema que se supervisa.
- Ver y establecer las acciones de recuperación automática del sistema (el temporizador de vigilancia del sistema operativo) del sistema que se supervisa.

  NOTA: Es posible que las opciones de recuperación automática del sistema no estén disponibles si el temporizador guardián del sistema operativo está habilitado en el BIOS. Para configurar las opciones de recuperación automática, el temporizador guardián del sistema operativo debe estar deshabilitado.

  NOTA: Es posible que las acciones de recuperación automática del sistema no se ejecuten exactamente conforme al tiempo de espera (n segundos) si el temporizador guardián identifica que el sistema ha dejado de responder. Los tiempos de ejecución de las acciones varían entre n-h+1 y n+1 segundos, siendo n el periodo del tiempo de espera y h el intervalo de latidos. El valor del intervalo de latidos es de 7 segundos cuando n ≤ 30 y de 15 segundos cuando n > 30.

  NOTA: No se puede garantizar que la función de temporizador guardián funcione correctamente si se produce un suceso incorregible relacionado con la memoria en el banco 1 de la DRAM del sistema. Si se produce un suceso incorregible relacionado con la memoria en esta ubicación, es posible que el código del BIOS residente en este espacio quede dañado. Ya que el temporizador guardián utiliza una llamada al BIOS para afectar al comportamiento de apagado o reinicio, es posible que esta función no funcione correctamente. En este caso, debe reiniciar el sistema manualmente. El temporizador guardián se puede configurar a un máximo de 720 segundos.

Apagado

Subfichas: Apagado remoto | Apagado térmico | Apagado de Web Server

En la ficha **Apagado**, se puede:

- Configurar las opciones de apagado del sistema operativo y de apagado remoto.
- Establecer el nivel de gravedad del apagado térmico para que apague el sistema en caso de que un sensor de temperatura envíe un valor de aviso o de error.

  NOTA: Un apagado térmico se produce solo cuando la temperatura informada por el sensor supera el umbral de temperatura. Este apagado no se produce si la temperatura informada es inferior al umbral de temperatura.
- Apagar el servicio de conexión de DSM SA (Web Server).

  NOTA: Server Administrator aún sigue disponible a través de la interfaz de la línea de comandos (CLI) cuando el servicio de conexión de DSM SA está apagado. Para usar las funciones de CLI no es necesario que el servicio de conexión de DSM SA esté en ejecución.

Registros

Subpestañas: Hardware | Alerta | Comando

En la pestaña **Registros**, se puede:

- Consultar el registro de Embedded System Management (ESM) o el registro de eventos del sistema (SEL) para obtener una lista de todos los sucesos relacionados con los componentes de hardware del sistema. El icono indicador de estado junto al nombre del registro cambia de estado normal () a estado no crítico () cuando el archivo de registro alcance el 80 por ciento de capacidad. En los sistemas PowerEdge de 11.ª generación, el icono indicador de estado junto al nombre del registro cambia a estado crítico () cuando el archivo de registro alcance el 100 por ciento de capacidad.

  NOTA: Habilitar la característica **Copia de seguridad automática y Borrar entradas de registro de ESM** le permite crear una copia de seguridad automática de los registros de ESM. Esta función solo está disponible en los servidores PowerEdge de 10.ª y 11.ª generación. El iDRAC ofrece funciones de eliminación automática de copia de seguridad y registro de SEL a partir de los servidores PowerEdge de 12.ª generación. En las ubicaciones mencionadas, solo está disponible la última versión del archivo XML de la copia de seguridad.
- Ver el registro de alertas para obtener una lista de todos los eventos generados por Server Administrator Instrumentation Service en respuesta a los cambios en el estado de los sensores y de otros parámetros supervisados.

  NOTA: Para obtener información acerca de cada identificación de evento de alerta y su descripción correspondiente, nivel de gravedad y causa, consulte la *Guía de referencia de mensajes de Server Administrator* en `dell.com/openmanagemanuals`.
- Ver el registro de comandos para obtener una lista de todos los comandos ejecutados desde la página de inicio de **Server Administrator** o desde su interfaz de línea de comandos.

  NOTA: Para obtener instrucciones para ver, imprimir, guardar y enviar registros por correo electrónico, consulte Registros de Server Administrator.

Administración de alertas

Subfichas: Acciones de alerta | Eventos de plataforma | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que el sensor de algún componente del sistema devuelva un valor de aviso o de error.
- Ver la conguración actual del filtro de eventos de plataforma y establecer las acciones del filtro de eventos de plataforma a realizar en caso de que el sensor de algún componente del sistema devuelva un valor de aviso o de error. Además, puede utilizar la opción **Configurar destino** para seleccionar un destino (dirección de IPv4 o IPv6) donde se envíe una alerta de evento de plataforma.

  NOTA: Server Administrator no muestra la id. de alcance de la dirección IPv6 en la interfaz gráfica de usuario.
- Ver los umbrales actuales de alerta de captura SNMP y establecer los niveles de umbral de alerta para componentes del sistema instrumentados. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.
  - **Captura de prueba SNMP** envía la captura para el destino seleccionado de la lista de destinos configurados que se muestra. El componente SNMP de Server Administrator debe estar instalado para poder enviar la captura de prueba. El administrador debe

configurar las direcciones IP/FQDN en el servicio de SNMP del sistema operativo o en un archivo de configuración para obtener la lista de destinos de captura.

NOTA: Esta función no se admite en VMware ESXi.

- **Activar capturas de SNMP** le permite configurar los valores para un componente mediante una casilla de verificación y un botón de opción. La selección de un botón de radio hace que cambie el estado apropiado de la casilla de marcación, mientras que deseleccionar el botón de radio también cambia el estado apropiado de la casilla de marcación.

NOTA: Las acciones de alerta de todos los sensores potenciales de componentes del sistema se enumeran en la ventana **Acciones de alerta**, incluso si no están presentes en el sistema. Configurar acciones de alerta para sensores de componentes del sistema que no estén presentes en el sistema no tiene ningún efecto.

NOTA: En todos los sistemas operativos Microsoft Windows, la opción **Configuración avanzada del sistema** > **Recuperación avanzada** del sistema operativo debe estar desactivada para garantizar que se generen las alertas de Server Administrator Automatic System Recovery.

Administración de sesiones

Subfichas: Sesión

En la ficha **Administración de sesiones**, puede:

- Ver información de la sesión de los usuarios actuales que han iniciado sesión en Server Administrator.
- Finalizar sesiones de usuarios.

NOTA: Solo los usuarios con privilegios de administrador pueden ver la página **Administración de sesiones** y finalizar las sesiones de los usuarios conectados.

Chasis del sistema principal o sistema principal

Haga clic en el objeto **Chasis del sistema principal** o **Sistema principal** para administrar los componentes de software y de hardware esenciales del sistema.

Los componentes que están disponibles son:

- Baterías
- BIOS
- Ventiladores
- Firmware
- Rendimiento del hardware
- Intrusión
- Memoria
- Red
- Puertos
- Administración de energía
- Fuentes de alimentación
- Procesadores
- Acceso remoto
- Medios flash extraíbles
- Ranuras
- Temperaturas
- Voltajes

NOTA: La opción **Fuentes de alimentación** no está disponible en PowerEdge 1900. Las funciones Supervisión de fuentes de alimentación y Supervisión de la alimentación solo están disponibles para aquellos sistemas que tengan dos o más suministros de

energía redundantes con capacidad de intercambio dinámico instaladas. Estas funciones no están disponibles para aquellos suministros de energía redundantes instalados de forma permanente que no dispongan de circuitería de administración de energía.

Propiedades del chasis del sistema principal o sistema principal

El módulo del servidor/sistema puede contener un chasis de sistema principal o varios chasis. El chasis del sistema principal/sistema principal contiene los componentes esenciales de un sistema. La ventana de acciones del objeto **Chasis del sistema principal/Sistema principal** incluye lo siguiente:

Propiedades

Subfichas: Condición | Información | Componentes del sistema (FRU)| Panel frontal

En la ficha **Propiedades**, se puede:

- Consultar la condición o el estado de los componentes del hardware y los sensores. Cada componente indicado tiene un icono de Indicadores de estado de los componentes del módulo del servidor/sistema junto a su denominación.  indica que la condición de un sistema es buena (normal).  indica que un componente tiene una condición de aviso (no crítica) y necesita una pronta atención.  indica que el componente tiene una condición de falla (crítica) y necesita atención inmediata.  indica que se desconoce el estado del componente. Entre los componentes supervisados disponibles se incluyen:
  - Baterías
  - Ventiladores
  - Registro de hardware
  - Intrusión
  - Red
  - Administración de energía
  - Fuentes de alimentación
  - Procesadores
  - Temperaturas
  - Voltajes

NOTA: Las baterías solo se admiten en sistemas PowerEdge de 10.ª generación. Las **Fuentes de alimentación** no están disponibles en PowerEdge 1900. La **Administración de energía** está admitida en un número limitado de sistemas PowerEdge de 10.ª generación. Las funciones **Supervisión de fuentes de alimentación** y **Supervisión de la alimentación** están disponibles solo para sistemas que tengan instaladas dos o más fuentes de alimentación redundantes con capacidad de intercambio dinámico. Estas funciones no están disponibles para suministros de energía no redundantes instalados de forma permanente y que no dispongan de circuitería de administración de energía.

NOTA: Si las tarjetas QLogic QLE2460 4Gb Single-Port Fibre Channel HBA, QLogic QLE2462 4Gb Dual-Port Fibre Channel HBA, Qlogic QLE2562 Dual Port FC8 Adapter o Qlogic QLE2560 Single Port FC8 Adapter están instaladas en sistemas PowerEdge de 12.ª generación, la pantalla **Componentes del sistema (FRU)** no aparece.

- Ver información sobre los atributos del chasis del sistema principal como el nombre de host, la versión de iDRAC, la versión de Lifecycle Controller, el modelo de chasis, el seguro del chasis, la etiqueta de servicio del chasis, el código de servicio rápido y la etiqueta de propiedad del chasis. El atributo Código de servicio rápido (ESC) es una conversión exclusivamente numérica de 11 dígitos de la etiqueta de servicio del sistema. Cuando llame a asistencia técnica de Dell EMC, puede introducir el ESC para el enrutamiento de llamada automático.
- Ver información detallada sobre las unidades reemplazables en el campo (FRU) que están instaladas en el sistema [en la subficha **Componentes del sistema** (**FRU**)].
- Habilitar o deshabilitar los botones del panel anterior del sistema administrado, como el botón Energía y el botón Interrupción sin enmascaramiento (NMI) (si están presentes en el sistema). Además, permite seleccionar el nivel de acceso de seguridad del LCD del sistema administrado. La información del LCD del sistema administrado se puede seleccionar en el menú desplegable. Puede además habilitar Indicación de sesión de KVM remoto desde la subficha **Panel frontal**.

Baterías

Haga clic en el objeto **Baterías** para ver la información de las baterías instaladas en el sistema. Las baterías conservan la fecha y la hora de apagado del sistema. La batería guarda la configuración del BIOS del sistema, lo que permite que el sistema se reinicie correctamente. La ventana de acciones del objeto Baterías puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

Subficha: baterías

En la ficha **Propiedades**, puede ver las lecturas actuales y el estado de las baterías del sistema.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la **ficha Administración de alertas**, puede

- Ver los valores actuales de las acciones de alerta.
- Configurar las alertas que desea que actúen en caso de un suceso crítico/de falla o de advertencia de la batería.

BIOS

Haga clic en el objeto **BIOS** para administrar características clave del BIOS del sistema. El BIOS del sistema contiene programas almacenados en un conjunto de chips de memoria flash que controlan la comunicación entre el microprocesador y los dispositivos periféricos, como el teclado y el adaptador de vídeo, además de otras funciones varias, como los mensajes del sistema. La ventana de acciones del objeto **BIOS** puede tener las siguientes fichas, dependiendo de los privilegios del grupo del usuario:

Propiedades y **Configuración**

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver la información del BIOS.

Configuración

Subficha: BIOS

NOTA: La ficha Configuración del BIOS del sistema solo muestra las funciones del BIOS compatibles con el sistema.

En la ficha **Configuración**, puede establecer el estado de cada objeto de configuración del BIOS.

Puede modificar el estado de diversas funciones de configuración del BIOS, incluidas, entre otras, el puerto serie, la secuencia de la unidad de disco duro, los puertos USB accesibles al usuario, la tecnología de virtualización de CPU, el Hyper-Threading de CPU, el modo de recuperación de corriente alterna, la controladora SATA incorporada, el perfil del sistema, la redirección de la consola y la velocidad en baudios a prueba de errores de la redirección de consola. Además, puede configurar el dispositivo USB interno, la configuración de la controladora de la unidad óptica, el temporizador guardián de la recuperación de sistema automática (ASR), el hipervisor incorporado y los puertos de red LAN adicionales en la información de la placa base. También puede ver la configuración del módulo de plataforma segura (TPM) y el módulo criptográfico seguro (TCM).

En función de la configuración específica del sistema, es posible que se muestren elementos de configuración adicionales. Sin embargo, en la pantalla Configuración del BIOS pueden mostrarse algunas opciones de configuración del BIOS que no son accesibles en Server Administrator.

En los sistemas PowerEdge de 12.ª generación y posteriores, las funciones configurables del BIOS se agrupan en categorías específicas. Las categorías incluyen Menú de depuración, Información del sistema, Configuración de la memoria, Configuración del procesador, Configuración de SATA, Configuración del inicio, Configuración de la opción de inicio, Inicio único, Configuración de la red, Dispositivos integrados, Desactivación de ranuras, Comunicación serie, Configuración de perfiles del sistema, Seguridad del sistema y Otros ajustes. Por ejemplo, en la página **Configuración del BIOS del sistema**, al hacer clic en el vínculo **Configuración de la memoria**, aparecen las funciones correspondientes a la memoria del sistema. Para ver o modificar la configuración, vaya a las categorías que corresponda.

NOTA: La categoría de inicio único no se admite en sistemas PowerEdge de 13.ª generación.

Las funciones configurables del BIOS se agrupan como categorías específicas. Las categorías incluyen Menú de depuración, Información del sistema, Configuración de la memoria, Configuración del procesador, Configuración de SATA, Configuración del inicio, Configuración de la opción de inicio, Configuración de la red, Dispositivos integrados, Desactivación de ranuras, Comunicación serie, Configuración de perfiles del sistema, Seguridad del sistema y Otros ajustes. Por ejemplo, en la página **Configuración del BIOS del sistema**, al hacer clic en el vínculo **Configuración de la memoria**, aparecen las funciones correspondientes a la memoria del sistema. Para ver o modificar la configuración, vaya a las categorías que corresponda.

Puede seleccionar una contraseña de configuración del BIOS en la página **Seguridad del sistema**. Si ha configurado la contraseña de configuración, introdúzcala para activar y modificar la configuración del BIOS. De lo contrario, la configuración del BIOS aparecerá en modo de solo lectura. Reinicie el sistema después de seleccionar la contraseña.

Cuando haya valores pendientes de la sesión anterior o se desactive la configuración en banda desde una interfaz fuera de banda, Server Administrator no permite la configuración del BIOS.

NOTA: La información de configuración de las tarjetas de interfaz de red (NIC) de la configuración del BIOS de Server Administrator puede ser imprecisa para las NIC incorporadas. Es posible que se produzcan resultados inesperados al utilizar la pantalla de configuración del BIOS para habilitar o deshabilitar NIC. Se recomienda realizar una configuración completa de las NIC incorporadas mediante la pantalla Configuración del sistema que aparece al presionar <F2> mientras el sistema se está iniciando.

Ciclo de encendido completo: esta nueva característica permitirá a los administradores del servidor realizar un ciclo de encendido del dispositivo mediante la GUI o la CLI de OpenManage. El **Ciclo de encendido completo** permite al administrador realizar un ciclo de encendido de corriente continua (CC) seguido de un ciclo de encendido de corriente alterna (CA).

Ciclo de encendido de CC: reinicia el servidor, pero los dispositivos auxiliares no se interrumpen.
Ciclo de encendido de CA: reinicia los dispositivos auxiliares y conecta al usuario al servidor.

El **Ciclo de encendido completo** incluye un ciclo de encendido de los siguientes dispositivos:

- Servidor
- BMC/iDRAC
- CPLD
- Sensores
- LCD
- Unidad reemplazable en la instalación
- Titan
- Tarjeta secundaria de red

Configuración del ciclo de encendido de CA virtual

Para configurar el ciclo de encendido de CA virtual:

1. En la ventana Server Administrator, expanda **Sistema** > **Chasis del sistema principal**.
2. Haga clic en **BIOS**.
   Aparece la ventana **Propiedades BIOS**.
3. Haga clic en la ficha **Configuración**.
   Se muestra la ventana **Configuración del BIOS del sistema**.
4. Haga clic en el vínculo **Otros ajustes**.
5. En **Solicitud del ciclo de encendido**, seleccione **CA virtual**.
6. Haga clic en **Aplicar**.

   NOTA: Reinicie el servidor para cambiar correctamente la configuración del ciclo de encendido.

Ventiladores

Haga clic en el objeto **Ventiladores** para administrar los ventiladores del sistema. Server Administrator supervisa el estado de cada ventilador del sistema a través de la medición de las rpm. Las sondas del ventilador le informan las rpm a Server Administrator Instrumentation Service.

Cuando selecciona Ventiladores en el árbol de dispositivos, se muestran los detalles en el área de datos del panel derecho de la página de inicio de Server Administrator. La ventana de acciones del objeto Ventiladores puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

Subficha: Sondas del ventilador

En la ficha **Propiedades**, se puede:

- Ver las lecturas actuales de las sondas de ventilador del sistema y configurar los valores mínimo y máximo para el umbral de advertencia de las sondas del ventilador.

  NOTA: Algunos campos de la sonda del ventilador difieren según el tipo de firmware que tenga el sistema, como BMC o ESM. Algunos valores de umbral no se pueden editar en sistemas basados en BMC.
- Seleccionar las opciones de control del ventilador.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que un ventilador devuelva un valor de advertencia o de error.
- Establecer los niveles de umbral de alerta para los ventiladores.

Firmware

Haga clic en el objeto **Firmware** para administrar el firmware del sistema. El firmware está compuesto por programas o datos que se han escrito en ROM. El firmware puede iniciar y operar un dispositivo. Cada controladora contiene un firmware que ayuda a proporcionar su funcionalidad. La ventana de acciones del objeto **Firmware** puede tener la siguiente ficha, según los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades** puede ver la información del firmware del sistema.

Rendimiento del hardware

Haga clic en el objeto **Rendimiento del hardware** para ver el estado y la causa de la degradación del rendimiento del sistema. La ventana de acciones del objeto **Rendimiento del hardware** puede tener la siguiente ficha, según los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver los detalles de la degradación de rendimiento del sistema.

La siguiente tabla enumera los valores posibles para el estado y la causa de una sonda:

Tabla 10. Valores posibles para el estado y causa de una sonda

Valores de estado	Valores de causa
Degraded	Configuración de usuario Capacidad de alimentación insuficiente Motivo desconocido
Normal	[N/A]

Intrusión

Haga clic en el objeto **Intrusión** para administrar el estado de intrusión en el chasis del sistema. Server Administrator supervisa el estado de intrusión como una medida de seguridad para impedir el acceso no autorizado a los componentes críticos del sistema. La intrusión en el chasis indica que se está abriendo o se ha abierto la cubierta del chasis del sistema. La ventana de acciones del objeto **Intrusión** puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**

Propiedades

Subficha: Intromisión

En la ficha **Propiedades**, se puede ver el estado de intrusión en el chasis.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que el sensor de intromisión devuelva un valor de aviso o de error.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para el sensor de intrusión. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

Memoria

Haga clic en el objeto **Memoria** para administrar los dispositivos de memoria del sistema. Server Administrator supervisa el estado del dispositivo de memoria para cada módulo de memoria presente en el sistema supervisado. Los sensores de fallas anteriores de dispositivos de memoria supervisan los módulos de memoria mediante un conteo del número de correcciones de memoria de ECC. Server Administrator supervisa además la información de redundancia de memoria si el sistema admite esta función. La ventana de acciones del objeto **Memoria** puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

Subficha: Memoria

En la ficha **Propiedades**, puede ver el estado de redundancia de memoria, los atributos de los arreglos de memoria, la capacidad total de los arreglos de memoria, los detalles de los arreglos de memoria, los detalles del dispositivo de memoria y el estado del dispositivo de memoria. Los detalles del dispositivo de memoria proporcionan los detalles de un dispositivo de memoria en un conector como el estado, el nombre de dispositivo, el tamaño, el tipo, la velocidad, el rango y los errores. Un rango es una hilera de dispositivos de memoria dinámica de acceso aleatorio (DRAM) que consta de 64 bits de datos por módulo de memoria en línea dual (DIMM). Los posibles valores de rango son `single, dual, quad, octal,hexa`. El rango muestra el rango de DIMM y ayuda en el servicio sencillo de DIMM en el servidor.

NOTA: Si un sistema con memoria de banco de reserva activada entra en un estado perdido de redundancia, es posible que no sea evidente cuál es el módulo de memoria con error. Si no puede determinar qué DIMM debe reemplazar, consulte el *conmutador* para la anotación de registro detectada del banco de memoria de reserva en el registro del sistema ESM para averiguar cuál es el módulo de memoria con error.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los ajustes actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que un módulo de memoria devuelva un valor de aviso o de error.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para los módulos de memoria. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

Red

Haga clic en el objeto**Red** para administrar la NIC del sistema. Server Administrator supervisa el estado de cada NIC presente en el sistema para asegurar la conexión remota continua. Server Administrator informa las capacidades de FCoE e iSoE de las NIC. Además, los detalles de asociación de NIC se informan si ya están configuradas en el sistema. Se puede asociar dos o más NIC físicas en una única NIC lógica, a la cual un administrador puede asignar una dirección IP. La asociación se puede configurar mediante las herramientas del proveedor de NIC. Por ejemplo, Broadcom - BACS. Si una de las NIC físicas presenta una falla, la dirección IP permanece accesible dado que está enlazada a la NIC lógica en lugar de a una única NIC física. Si la interfaz de asociación está configurada, se muestran los detalles de las propiedades de la asociación. También se informa la relación entre las NIC físicas y la interfaz de asociación y viceversa si estas NIC físicas son miembros de la interfaz de asociación.

En el sistema operativo Windows 2008 Hypervisor, Server Administrator no informa las direcciones IP de los puertos NIC físicos que se usan para asignar una IP a una máquina virtual.

NOTA: No se garantiza que el orden en el que se detectan los dispositivos coincidirá con el orden de puertos físicos del dispositivo. Haga clic en el hipervínculo de Nombre de la interfaz para consultar información sobre la tarjeta de interfaz de red (NIC).

En el caso de sistemas operativos ESXi, el dispositivo de red se considera como un grupo. Por ejemplo, la interfaz de Ethernet virtual que usa la consola de servicios (vswif) y la interfaz de red virtual que usan los dispositivos vmknic en ESXi.

NOTA: Server Administrator solo admite inventario de interfaces físicas de red y sus propiedades. Server Administrator no admite inventario de interfaces lógicas como VLAN e interfaces de túnel.

La ventana de acciones del objeto **Red** puede tener la siguiente ficha, en función de los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver información sobre las interfaces de NIC física y también sobre las interfaces de asociación instaladas en el sistema.

NOTA: En la sección Direcciones IPv6, Server Administrator muestra solo dos direcciones además de la dirección de vínculo local.

NOTA: En los sistemas que ejecutan sistemas operativos Linux con versiones de kernel anteriores a 3.10, no se muestra la velocidad de la interfaz de asociación.

Puertos

Haga clic en el objeto **Puertos** para administrar los puertos externos del sistema. Server Administrator supervisa el estado de cada puerto externo presente en el sistema.

NOTA: Server Administrator no enumera los puertos USB de CMC conectados a los servidores blade.

La ventana de acciones del objeto **Puertos** puede tener la siguiente ficha, dependiendo de los privilegios de grupo del usuario: **Propiedades**.

Subficha: Información

Propiedades

En la ficha **Propiedades**, puede ver información sobre los puertos internos y externos del sistema.

Administración de energía

NOTA: Las funciones Supervisión de fuentes de alimentación y Supervisión de la alimentación están disponibles solo para sistemas que tengan instaladas dos o más fuentes de alimentación redundantes con capacidad de intercambio dinámico. Estas funciones no están disponibles para suministros de energía no redundantes instalados de forma permanente y que no dispongan de circuitería de administración de energía.

Supervisión

Subfichas: Consumo | Estadísticas

La ficha **Consumo** permite ver y administrar la información sobre consumo de energía del sistema, expresada en vatios y BTU/h.

BTU/h= vatio X 3,413 (valor redondeado al número entero más cercano)

Server Administrator supervisa el estado del consumo de energía y el amperaje, y lleva un registro de los detalles estadísticos de la alimentación.

Puede además ver la capacidad de aumento instantánea del sistema y la capacidad de aumento pico del sistema. Los valores se muestran en vatios y BTU/h (unidad térmica británica). Los umbrales de alimentación se pueden establecer en vatios y BTU/h.

La ficha Estadísticas permite ver y restablecer las estadísticas de seguimiento de alimentación del sistema, como el consumo de energía, la potencia pico del sistema y el amperaje pico del sistema.

Administración

Subfichas: Presupuesto | Perfiles

La ficha **Presupuesto** le permite ver los atributos del inventario de alimentación como alimentación inactiva del sistema y potencial máximo de alimentación del sistema en vatios y BTU/h. Puede también usar la opción Presupuesto de alimentación para activar la capacidad de alimentación y establecer la capacidad de alimentación para el sistema.

La ficha **Perfiles** permite elegir un perfil de alimentación para maximizar el rendimiento del sistema y ahorrar energía.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

Utilice la ficha **Acciones de alerta** para definir acciones de alerta del sistema para diversos eventos como Aviso de sonda de alimentación del sistema y Alimentación pico del sistema.

Utilice la ficha **Capturas SNMP** para configurar este tipo de capturas para el sistema.

Es posible que determinadas funciones de administración de energía solo estén disponibles en los sistemas activados con el bus de administración de energía (PMBus).

Fuentes de alimentación

Haga clic en el objeto **Suministros de energía** para administrar los suministros de energía del sistema. Server Administrator supervisa el estado del suministro de energía, incluyendo la redundancia, para garantizar que cada suministro de energía presente en el sistema funciona correctamente.

La ventana de acciones del objeto Suministros de energía puede incluir las siguientes fichas según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

NOTA: Las funciones Supervisión de fuentes de alimentación y Supervisión de la alimentación solo están disponibles para aquellos sistemas que tengan dos o más suministros de energía redundantes con capacidad de intercambio dinámico instaladas. Estas funciones no están disponibles para aquellos suministros de energía redundantes instalados de forma permanente que no dispongan de circuitería de administración de energía.

Propiedades

Subficha: Elementos

En la ficha **Propiedades**, se puede:

- Ver información sobre los atributos de redundancia de los suministros de energía.
- Verificar el estado de los elementos del suministro de energía individuales, incluso la versión de firmware del suministro de energía y la potencia de salida máxima.
- Verificar el estado de los elementos del suministro de energía individuales, incluso la versión de firmware del suministro de energía, la potencia de entrada nominal y la potencia de salida máxima. El atributo de vatios nominales de entrada se muestra solo en los sistemas PMBus a partir de la 11.ª generación.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha Administración de alertas, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que la alimentación de un sistema genere un valor de advertencia o de error.
- Configurar destinos de alertas de sucesos de plataforma para direcciones IPv6.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para los vatios de alimentación del sistema. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

NOTA: La captura de alimentación pico del sistema solo genera sucesos para el nivel de gravedad informativo.

Procesadores

Haga clic en el objeto **Procesadores** para administrar los microprocesadores del sistema. El procesador es el chip informático principal que se encuentra dentro del sistema y que controla la interpretación y la ejecución de las funciones aritméticas y lógicas. La ventana de acciones del objeto Procesadores puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Subficha: Información

Propiedades

En la ficha **Propiedades**, puede ver información sobre los microprocesadores del sistema y acceder a información detallada de capacidades y caché.

Administración de alertas

Subfichas: Acciones de alertas

En la ficha **Administración de alertas**, puede ver los valores de las acciones de alerta actuales y establecer las acciones de alerta que desea que se realicen en caso de que un procesador devuelva un valor de aviso o de error.

Acceso remoto

Haga clic en el objeto **Acceso remoto** para administrar las funciones de la controladora de administración de la placa base (BMC) o del Integrated Dell Remote Access Controller (iDRAC) y del Remote Access Controller (RAC).

Seleccionar la ficha Acceso remoto le permite administrar las funciones de BMC/iDRAC como la información general de BMC/iDRAC. También puede administrar la configuración de BMC/iDRAC en una red de área local (LAN), el puerto serie para BMC/iDRAC, la configuración del modo de terminal del puerto serie, BMC/iDRAC en una conexión de comunicación en serie en la LAN y los usuarios de BCM/iDRAC.

NOTA: Si una aplicación que no sea Server Administrator se usa para configurar BMC/iDRAC a la vez que se ejecuta Server Administrator, es posible que los datos de la configuración de BMC/iDRAC que muestra Server Administrator se vuelvan asincrónicos

con BMC/iDRAC. Se recomienda que Server Administrator se utilice para configurar BMC/iDRAC mientras se ejecuta Server Administrator.

DRAC le permite acceder a las capacidades de administración remota del sistema. DRAC de Server Administrator proporciona acceso remoto a los sistemas que no funcionan, notificaciones de alerta cuando el sistema no responde y la capacidad de reiniciar el sistema.

La ventana de acciones del objeto **Acceso remoto** puede tener las siguientes fichas, dependiendo de los privilegios de grupo del usuario: **Propiedades**, **Configuración** y Usuarios.

Subficha: Información

Propiedades

En la ficha **Propiedades**, puede ver la información general sobre el dispositivo de acceso remoto. Es posible también ver los atributos de las direcciones IPv4 e IPv6.

Haga clic en **Restablecer valores predeterminados** para restablecer todos los atributos a los valores predeterminados del sistema.

Subfichas: LAN | Puerto serie | Comunicación en serie en la LAN |Configuración adicional

Configuración

En la ficha Configuración, cuando BMC/iDRAC están configurados, puede configurar BMC/iDRAC en una LAN, el puerto serie para BMC/iDRAC y BMC/iDRAC en una comunicación en serie en la LAN.

NOTA: La ficha Configuración adicional solo está disponible en sistemas con iDRAC.

Cuando DRAC está configurada, la ficha **Configuración** le permite establecer las propiedades de red.

En la ficha **Configuración adicional**, puede activar o desactivar las propiedades IPv4/IPv6.

NOTA: La activación o desactivación de IPv4/IPv6 solo es posible en un entorno de doble pila (donde ambas pilas IPv4 e IPv6 están cargadas).

Usuarios

Subficha: Usuarios

En la ficha **Usuarios**, puede modificar la configuración de usuario de acceso remoto. Puede agregar, configurar y ver información sobre los usuarios de Remote Access Controller.

Medios flash extraíbles

Haga clic en el objeto **Medios flash extraíbles** para ver la condición y el estado de redundancia de los módulos SD internos y los medios vFlash. La ventana de acciones **Medios flash extraíbles** tiene la ficha **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver la información sobre los medios flash extraíbles y los módulos SD internos. Incluye detalles sobre el nombre del conector, su estado y el tamaño del almacenamiento.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen si la sonda de unidades flash extraíbles devuelve un valor de aviso o de error.
- Ver los umbrales actuales de alertas de captura SNMP y establecer los niveles de umbral de alerta para las sondas de medios flash extraíbles. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

La administración de alertas es común para los módulos SD internos y vFlash. La configuración de acciones de alerta, SNMP, PEF para los módulos SD o vFlash establece automáticamente uno para el otro.

Ranuras

Haga clic en el objeto **Ranuras** para administrar los conectores o enchufes de la placa del sistema que aceptan placas de circuito impreso, como tarjetas de expansión. La ventana de acciones del objeto Ranuras tiene una ficha **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver información sobre todas las ranuras y adaptadores instalados.

Temperaturas

Haga clic en el objeto **Temperaturas** para administrar la temperatura del sistema a fin de evitar daños térmicos en los componentes internos del sistema. Server Administrator supervisa la temperatura en varias ubicaciones del chasis del sistema para garantizar que las temperaturas del interior del chasis no suban demasiado.

La ventana de acciones del objeto **Temperaturas** muestra las siguientes fichas según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Subficha: Sondas de temperatura

En la ficha **Propiedades**, puede ver las lecturas actuales y estados de las sondas de temperatura del sistema y configurar valores mínimos y máximos para el umbral de advertencia de sonda de temperatura.

NOTA: Algunos campos de sondas de temperatura difieren según el tipo de firmware que tenga el sistema, como BMC o ESM. Algunos valores de umbral no se pueden editar en sistemas basados en BMC. Al asignar valores de umbrales de sonda, Server Administrator a veces redondea los valores mínimos o máximos introducidos al valor asignable más cercano.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que una sonda de temperatura devuelva un valor de advertencia o de error.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para las sondas de temperatura. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

NOTA: Puede establecer valores mínimos y máximos para los umbrales de sondas de temperatura para un chasis externo en números enteros solamente. Si intenta establecer el valor mínimo o máximo para el umbral de sonda de temperatura en un número que contiene un décimal, solo se guardará el número entero anterior al lugar del decimal como el valor del umbral.

Voltajes

Haga clic en el objeto **Voltajes** para administrar los niveles de voltaje del sistema. Server Administrator supervisa los voltajes de los componentes críticos en varias ubicaciones del chasis del sistema supervisado. La ventana de acciones del objeto **Voltajes** puede tener las siguientes fichas, según los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

Subficha: Sondas de voltaje

En la ficha **Propiedades** puede ver las lecturas actuales y estados de las sondas de voltaje del sistema, y configurar valores mínimos y máximos para el umbral de aviso de la sonda de voltaje.

NOTA: Algunos campos de sonda de voltaje difieren en función del tipo de firmware que tiene el sistema, como BMC o ESM. Algunos valores de umbral no se pueden editar en sistemas basados en BMC.

Administración de alertas

Subfichas: Acciones de alerta | Capturas SNMP

En la ficha **Administración de alertas**, puede:

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que un sensor de voltaje del sistema devuelva un valor de aviso o de error.
- Ver los umbrales de alerta de capturas SNMP y establecer los niveles de umbral de alerta para los sensores de voltaje. Las capturas seleccionadas se desencadenan si el sistema genera un evento que corresponda en el nivel de gravedad seleccionado.

Software

Haga clic en el objeto **Software** para ver la información detallada de la versión sobre los componentes esenciales del software del sistema administrado, como el sistema operativo y el software de administración de sistemas. La ventana de acciones del objeto Software tiene la siguiente ficha, según los privilegios de grupo del usuario: **Propiedades**.

Subficha: Resumen

Propiedades

En la ficha **Propiedades**, puede ver un resumen del sistema operativo del sistema supervisado y el software de administración de sistemas.

Sistema operativo

Haga clic en el objeto **Sistema operativo** para ver la información básica sobre el sistema operativo. La ventana de acciones del objeto Sistema operativo tiene la siguiente ficha, según los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Información

En la ficha **Propiedades**, puede ver información básica sobre el sistema operativo.

Almacenamiento

Server Administrator proporciona Storage Management Service:

Storage Management Service proporciona funciones para configurar dispositivos de almacenamiento. En la mayoría de los casos, Storage Management Service se instala con **Configuración típica**. Storage Management Service está disponible en los sistemas operativos Microsoft Windows, Red Hat Enterprise Linux y SUSE Linux Enterprise Server.

Cuando Storage Management Service esté instalado, haga clic en el objeto **Almacenamiento** para ver el estado y la configuración de diversos dispositivos de almacenamiento de arreglo conectados, discos del sistema, etc.

En el caso de Storage Management Service, la ventana de acciones del objeto Almacenamiento tiene la siguiente ficha, según los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Estado

En la ficha **Propiedades**, puede ver el estado o condición de los sensores y los componentes de almacenamiento conectados, como los subsistemas de arreglos y los discos del sistema operativo.

Administración de preferencias: opciones de configuración de la página de inicio

El panel izquierdo de la página de inicio **Preferencias** (donde se muestra el árbol del sistema en la página de inicio de Server Administrator) muestra todas las opciones de configuración disponibles en la ventana del árbol del sistema. Las opciones que se muestran se basan en el software de administración de sistemas instalado en el sistema administrado.

Las opciones de configuración disponibles de la página de inicio **Preferencias** son las siguientes:

- Configuración general
- Administrador del servidor

Configuración general

Haga clic en el objeto **Configuración general** para configurar las preferencias de usuario y el servicio de conexión del DSM SA (Web Server) para ciertas funciones de Server Administrator. La ventana de acciones del objeto Configuración general tiene las siguientes fichas, en función de los privilegios del grupo del usuario: **Usuario** y **Web Server**.

Subficha: Propiedades

Usuario

En la ficha **Usuario**, puede establecer las preferencias de usuario, como la apariencia de la página de inicio y la dirección de correo electrónico predeterminada para el botón **Correo electrónico**.

- **Servidor web**
- **Subfichas: Propiedades | Certificado X.509**

En la ficha Web Server, puede:

- Configurar las preferencias del servicio de conexión del DSM SA. Para obtener instrucciones acerca de cómo configurar las preferencias del servidor, consulte Configuración de la seguridad y del servicio de conexión de administración de servidores de Dell EMC Systems Management.
- Configurar la dirección del servidor SMTP y la dirección IP de enlace ya sea en el modo de dirección IPv4 o IPv6.
- Para administrar el certificado X.509, genere un nuevo certificado X.509, utilice nuevamente un certificado X.509 existente o importe una cadena de certificados de una entidad de certificación (CA). Para obtener más información sobre la administración de certificados, consulte Administración de certificados X. 509.

Administrador del servidor

Haga clic en el objeto **Server Administrator** para activar o desactivar el acceso de usuarios con privilegios de usuario o usuario avanzado. La ventana de acciones del objeto **Server Administrator** puede tener la siguiente ficha, según los privilegios de grupo del usuario: **Preferencias**.

Subficha: Configuración de acceso

Preferencias

En la ficha **Preferencias** puede activar o desactivar el acceso de los usuarios con privilegios de usuario o de usuario avanzado.

5

Registros de Server Administrator

Server Administrator le permite ver y administrar los registros de hardware, alertas y comandos. Todos los usuarios pueden acceder a los registros e imprimir informes desde la página de inicio de Server Administrator o desde su interfaz de línea de comandos. Los usuarios deben iniciar sesión con privilegios de administrador para borrar los registros o deben iniciar sesión con privilegios de administrador o usuario avanzado para enviar registros por correo electrónico al contacto de servicio designado.

Para obtener más información sobre la visualización de registros y la creación de informes desde la línea de comandos, consulte la *Guía de la interfaz de línea de comandos de Server Administrator* en **dell.com/openmanagemanuals**.

Al ver los registros de Server Administrator, puede hacer clic en **Ayuda** () para obtener información más detallada sobre la ventana específica que esté viendo. La ayuda del registro de Server Administrator está disponible para todas las ventanas a las que el usuario puede acceder según el nivel de privilegio del usuario y los grupos de hardware y software específicos que Server Administrator descubre en el sistema administrado.

Temas:

Funciones integradas

Haga clic en el encabezado de una columna para organizar por columna o para cambiar la dirección del ordenamiento de la columna. Además, cada ventana de registro contiene varios botones de tareas que se pueden utilizar para administrar y ofrecer asistencia al sistema.

Botones de tareas de la ventana de registro

La siguiente tabla enumera los botones de tareas de la ventana de registro.

Tabla 11. Botones de tareas de la ventana de registro

Nombre	Descripción
Imprimir	Para imprimir una copia del registro en la impresora predeterminada.
Exportar	Para guardar un archivo de texto que contiene los datos de registro (con los valores de cada campo de datos separados mediante un delimitador a elegir) en el destino que desee.
Correo electrónico	Para crear un mensaje de correo electrónico que incluya el contenido del registro como un archivo adjunto.
Borrar registro	Para eliminar todos los eventos del registro.
Guardar como	Para guardar el contenido del registro en un archivo `.zip`.
Actualizar	Para volver a cargar el contenido del registro en el área de datos de una ventana de acciones.

NOTA: Para obtener información adicional sobre cómo utilizar los botones de tareas, consulte Botones de tareas.

Registros de Server Administrator

Server Administrator proporciona los siguientes registros:

- Registro de hardware
- Registro de alertas
- Registro de comandos

Registro de hardware

En los sitemas PowerEdge de 11.ª generación, use el registro de hardware para localizar posibles problemas con los componentes del hardware del sistema. El indicador de estado del registro de hardware cambia a estado crítico () cuando el archivo de registro alcanza el 100 por ciento de capacidad. Hay dos registros de hardware disponibles, en función del sistema: el registro de Embedded System Management (ESM) y el registro de eventos del sistema (SEL). El registro de ESM y el SEL son conjuntos individuales de instrucciones incorporadas que pueden enviar mensajes de estado del hardware a Systems Management Software. Cada componente enumerado en los registros tiene un icono indicador de estado junto a su nombre. En la siguiente tabla se muestran los indicadores de estado.

Tabla 12. Indicadores de estado del registro de hardware

Estado	Descripción
Una marca de verificación verde ()	indica que el componente se encuentra en buen estado (normal).
Un triángulo de color amarillo que contiene un punto de exclamación ()	indica que el componente presenta una condición de aviso (no crítica) y necesita una pronta atención.
Una X roja ()	indica que el componente presenta una condición crítica/de error y requiere atención inmediata.
Un signo de interrogación ()	indica que el estado del componente es desconocido.

Para acceder al registro de hardware, haga clic en **Sistema**, en la ficha **Registros** y, a continuación, en **Hardware**.

La información que aparece en los registros ESM y SEL incluye:

- El nivel de gravedad del evento
- La fecha y hora en la que se capturó el evento
- Una descripción del evento

Mantenimiento del registro de hardware

El ícono de indicador de estado que se encuentra junto al nombre del registro en la página de inicio de Server Administrator pasa del estado normal () al estado no crítico () cuando el archivo de registro alcanza 80 por ciento de la capacidad. Asegúrese de borrar el registro de hardware cuando alcance el 80 por ciento de la capacidad. Si el registro tiene permitido alcanzar una capacidad del 100 por ciento, se descartan los últimos eventos del registro.

Para borrar un registro de hardware, en la página **Registro de hardware**, haga clic en el vínculo **Borrar registro**.

Registro de alertas

NOTA: Si el registro de alertas muestra datos XML no válidos (por ejemplo, cuando los datos XML generados para la selección no están bien formados), haga clic en **Borrar registro** y vuelva a visualizar la información del registro.

NOTA: El tamaño del archivo de registro de alertas está limitado. Para capturar el máximo de registros de alertas, habilite todos los filtros de registro del sistema operativo.

Use el registro de alertas para supervisar distintos eventos del sistema. Server Administrator genera eventos en respuesta a los cambios en el estado de los sensores y a otros parámetros supervisados. Cada evento de cambio de estado registrado en el registro de alertas consta de un identificador único denominado ID de evento para una categoría de fuente de evento específica y un mensaje de evento que lo describe. El ID de evento y el mensaje describen exclusivamente la gravedad y causa del evento y proporcionan otra información relevante como la ubicación del evento y el estado anterior del componente supervisado.

Para acceder al registro de alertas, haga clic en **Sistema**, en la pestaña **Registros** y, a continuación, en **Alerta**.

La información que aparece en el registro de alertas incluye:

- El nivel de gravedad del evento
- El ID del evento
- La fecha y hora en la que se capturó el evento

- La categoría del evento
- Una descripción del evento

NOTA: Es posible que el historial del registro se requiera para la solución de problemas y realización de diagnósticos en el futuro. Por lo tanto, se recomienda guardar los archivos de registro.

NOTA: OMSA puede enviar capturas de SNMP duplicadas o registrar eventos duplicados en la página Registro de alertas o en el archivo de registro del sistema operativo. Las capturas y los eventos duplicados se registran cuando los servicios de OMSA se reinician manualmente o cuando el sensor del dispositivo aún indica un estado no normal cuando los servicios de OMSA se inician después de un reinicio del sistema operativo.

Para obtener información detallada sobre los mensajes de alertas, consulte la *Guía de referencia de mensajes de Server Administrator* en **dell.com/openmanagemanuals**.

Registro de comandos

NOTA: Si el registro de comandos muestra datos XML no válidos (por ejemplo, cuando los datos XML generados para la selección no están bien formados), haga clic en **Borrar registro** y vuelva a mostrar la información del registro.

Utilice el registro de comandos para supervisar todos los comandos que emiten los usuarios de Server Administrator. El registro de comandos realiza el seguimiento de los inicios de sesión, los cierres de sesión, la inicialización del software de administración de sistemas, el apagado iniciado por el software de administración de sistemas y deja constancia de la última vez que se borró el registro. El tamaño del archivo de registro de comandos se puede especificar según sus requisitos.

Para acceder al registro de comandos, haga clic en **Sistema**, **Registros** y, a continuación, haga clic en **Comando**.

La información que aparece en el registro de comandos incluye:

- La fecha y hora en la que se invocó el comando
- El usuario que está conectado en ese momento a la página de inicio de Server Administrator o a la CLI
- Una descripción del comando y los valores correspondientes

NOTA: Es posible que el historial del registro se requiera para la solución de problemas y realización de diagnósticos en el futuro. Por lo tanto, se recomienda guardar los archivos de registro.

6

Uso de Remote Access Controller

El controlador de administración de placa base (BMC)/Integrated Dell Remote Access Controller (iDRAC) supervisa el sistema en busca de sucesos críticos, para lo que se comunica con diversos sensores de la placa de sistema y envía alertas y registra sucesos cuando ciertos parámetros superan los umbrales preconfigurados. El BMC/iDRAC admite la especificación de la interfaz de administración de plataforma inteligente (IPMI) estándar del sector, lo que le permite configurar, supervisar y recuperar sistemas de forma remota.

NOTA: El Integrated Dell Remote Access Controller (iDRAC) se admite en los sistemas PowerEdge de 10.ª generación y posteriores.

El DRAC es una solución de hardware y software para administración de sistemas diseñada para proporcionar funciones de administración remota, recuperación de sistemas bloqueados y control de alimentación para sistemas.

Gracias a la comunicación con el controlador de administración de placa base (BMC)/Integrated Dell Remote Access Controller (iDRAC) del sistema, el DRAC puede configurarse para enviar alertas por correo electrónico en caso de avisos o errores relacionados con voltajes, temperaturas y velocidades de ventiladores. El DRAC también registra los datos de los sucesos y la última pantalla de falla (disponible solamente en los sistemas que ejecuten un sistema operativo Microsoft Windows) para ayudarle a diagnosticar la causa probable de una falla del sistema.

Remote Access Controller proporciona acceso remoto a un sistema que no funciona, lo que le permite poner el sistema en funcionamiento lo más rápido posible. Remote Access Controller también envía notificaciones de alerta cuando un sistema se encuentra inactivo y le permite reiniciar el sistema de forma remota. Además, Remote Access Controller registra la posible causa de las fallas del sistema y guarda la *pantalla de bloqueo más reciente*.

Puede iniciar sesión en Remote Access Controller mediante la página de inicio de Server Administrator o accediendo directamente a la dirección IP de la controladora usando un explorador compatible.

Al utilizar Remote Access Controller, puede hacer clic en **Ayuda** para obtener información más detallada sobre la ventana específica que esté visualizando. La ayuda de Remote Access Controller está disponible para todas las ventanas accesibles al usuario según el nivel de privilegio del usuario y los grupos específicos de hardware y software que Server Administrator descubre en el sistema administrado.

NOTA: Para obtener más información sobre el BMC, consulte la *Guía del usuario del controlador de administración de placa base Dell EMC OpenManage* en `dell.com/systemsecuritymanuals`.

NOTA: Para obtener información detallada sobre la configuración y el uso de iDRAC, consulte la *Guía del usuario de Integrated Dell Remote Access Controller* en `dell.com/systemsecuritymanuals`.

La siguiente tabla enumera los nombres de campo de la interfaz gráfica de usuario (GUI) y el sistema al que se aplica, cuando se instala Server Administrator en el sistema.

Tabla 13. Nombres de campo de la interfaz gráfica de usuario y el sistema al que se aplica

Nombre de campo de la interfaz gráfica de usuario	Sistema al que se aplica
Gabinete modular	Sistema modular
Módulos del servidor	Sistema modular
Sistema principal	Sistema modular
Sistema	Sistema no modular
Chasis del sistema principal	Sistema no modular

Para obtener más información sobre la compatibilidad de los sistemas con dispositivos de acceso remoto, consulte la *Matriz de compatibilidad de software de los sistemas Dell EMC* disponible en **dell.com/openmanagemanuals**.

Server Administrator permite acceso remoto en banda a registros de sucesos, control de alimentación e información de estado de sensores, y permite configurar el BMC/iDRAC. Para administrar el BMC/iDRAC y el DRAC mediante la interfaz gráfica de usuario (GUI) de Server Administrator, haga clic en el objeto **Acceso remoto**, que es un subcomponente del grupo **Chasis del sistema principal/ Sistema principal**.

Es posible puede realizar las siguientes tareas:

- Visualización de la información básica

- Configuración del dispositivo de acceso remoto para usar una conexión LAN
- Configuración del dispositivo de acceso remoto para usar una comunicación en serie en la LAN
- Configuración del dispositivo de acceso remoto para usar una conexión de puerto serie
- Configuración adicional para iDRAC
- Configuración de usuarios del dispositivo de acceso remoto
- Establecimiento de alertas de filtro para eventos de plataforma

Puede ver la información relacionada con BMC/iDRAC o DRAC, de acuerdo con el hardware que proporciona las capacidades de acceso remoto del sistema.

Los informes y la configuración del BMC/iDRAC y el DRAC también se pueden administrar mediante el comando `omreport/omconfig chassis remoteaccess` de la interfaz de la línea de comandos (CLI).

Además, Server Administrator Instrumentation Service permite administrar los parámetros de los filtros de eventos de plataforma (PEF) y los destinos de las alertas.

Temas:

Visualización de la información básica

Puede ver información básica sobre BMC/iDRAC, la dirección IPv4 y DRAC. Asimismo, puede restablecer la configuración de la controladora de acceso remoto a los valores predeterminados. Para hacerlo:

NOTA: Debe estar conectado con privilegios de administrador para restablecer la configuración de BMC.

Haga clic en **Gabinete modular** > **Módulo del servidor/sistema** > **Chasis del sistema principal/Sistema principal** > **Acceso remoto**

La página **Acceso remoto** muestra la siguiente información básica de la BMC del sistema:

Dispositivo de acceso remoto

- Tipo de dispositivo
- Versión de IPMI
- GUID del sistema
- Número de sesiones activas posibles
- Número actual de sesiones activas
- LAN activada
- Comunicación en serie en la LAN activada
- Dirección MAC

Dirección IPv4

- Fuente de dirección IP
- Dirección IP
- Subred IP
- Puerta de enlace IP

Dirección IPv6

- Fuente de dirección IP
- Dirección IPv6 1
- Puerta de enlace predeterminada
- Dirección IPv6 2
- Dirección local de vínculo
- Fuente de dirección DNS

- Servidor DNS preferido
- Servidor DNS alternativo

NOTA: Solo puede ver la información detallada de las direcciones IPv4 e IPv6 si activa las propiedades de dirección IPv4 e IPv6 en la sección **Configuración adicional** en la ficha **Acceso remoto**.

Configuración del dispositivo de acceso remoto para usar una conexión LAN

Para configurar el dispositivo de acceso remoto para comunicarse a través de una conexión LAN:

1. Haga clic en el objeto **Gabinete modular** > **Módulo del servidor/sistema** > **Chasis del sistema principal/Sistema principal** > **Acceso remoto**.
2. Haga clic en la pestaña **Configuración**.
3. Haga clic en **LAN**.

   Aparecerá la ventana **Configuración de la LAN**.

   NOTA: El tráfico de administración de BMC/iDRAC no funcionará correctamente si la LAN de la placa base (LOM) se asocia con tarjetas complementarias de adaptador de red.

4. Configure los siguientes detalles en la configuración de la NIC:
   - Activar NIC (seleccione esta opción para la asociación de NIC).

   NOTA: DRAC contiene una NIC 10BASE-T/100BASE-T Ethernet integrada y admite TCP/IP. La dirección predeterminada de NIC es 192.168.20.1 y la puerta de enlace predeterminada es 192.168.20.1.

   NOTA: Si se configura DRAC con la misma dirección IP que otra NIC en la misma red, habrá un conflicto de direcciones IP. DRAC dejará de responder a los comandos de la red hasta que se cambie la dirección IP en DRAC. Se debe restablecer DRAC incluso si el conflicto de direcciones IP se resuelve cuando se cambia la dirección IP de la otra NIC.

   NOTA: DRAC se restablece cuando se cambia su dirección IP. Si SNMP realiza un sondeo de DRAC antes de que se inicialice, se registra una advertencia de temperatura dado que la temperatura correcta no se transmite hasta que DRAC se inicialice.
   - Selección de NIC

   NOTA: La opción Selección de NIC no puede configurarse en sistemas modulares.

   NOTA: La opción Selección de NIC solo está disponible en los sistemas de 11.ª generación y versiones anteriores.

   - Opciones de red primaria y de conmutación por error

   Para los sistemas de 12.ª generación, las opciones de red primaria para `NIC` de administración remota (iDRAC7) son: `LOM1`, `LOM2`, `LOM3`, `LOM4` y `Dedicado`. Las opciones de red de conmutación por error son las siguientes: `LOM1`, `LOM2`, `LOM3`, `LOM4`, `Todos los LOM` y `Ninguno`.

   NOTA: La opción `Dedicado` está disponible cuando la licencia Enterprise de iDRAC7 está presente y es válida.The número de LOM varía según la configuración del sistema o del hardware.

   - Activar la IPMI en la LAN
   - Fuente de dirección IP
   - Dirección IP
   - Máscara de subred
   - Dirección de puerta de enlace
   - Límite del nivel de privilegios del canal
   - Nueva clave de cifrado
5. Configure los siguientes detalles opcionales de la configuración de la VLAN:

   NOTA: La configuración de VLAN no se puede aplicar en los sistemas con iDRAC.

   - Habilitar identificación de VLAN
   - ID de VLAN
   - Prioridad

6. Configure las siguientes propiedades de IPv4:
   - Fuente de dirección IP
   - Dirección IP
   - Máscara de subred
   - Dirección de puerta de enlace
7. Configure las siguientes propiedades de IPv6:
   - Fuente de dirección IP
   - Dirección IP
   - Longitud del prefijo
   - Puerta de enlace predeterminada
   - Fuente de dirección DNS
   - Servidor DNS preferido
   - Servidor DNS alternativo

   NOTA: Solo puede configurar la información detallada de las direcciones IPv4 e IPv6 si activa las propiedades de IPv4 e IPv6 en **Configuración adicional**.
8. Haga clic en **Aplicar cambios**.

Configuración del dispositivo de acceso remoto para usar una conexión de puerto serie

Para configurar la BMC para comunicaciones a través de una conexión de puerto serie:

1. Haga clic en **Gabinete modular** > **Módulo del servidor/sistema** > **Chasis del sistema principal/Sistema principal** > **Acceso remoto**.
2. Haga clic en la ficha **Configuración**.
3. Haga clic en **Puerto serie**.

   Aparecerá la ventana **Configuración del puerto serie**.
4. Configure los siguientes detalles:
   - Configuración del modo de conexión
   - Velocidad en baudios
   - Control de flujo
   - Límite del nivel de privilegios del canal
5. Haga clic en **Aplicar cambios**.
6. Haga clic en **Configuración del modo de terminal**.

   En la ventana Configuración del modo de terminal, puede configurar los valores del modo de terminal para el puerto serie.

   El modo de terminal se utiliza para el envío de mensajes de administración de interfaz de plataforma inteligente (IPMI) a través del puerto serie con caracteres ASCII imprimibles. El modo de terminal también es compatible con un número limitado de comandos de texto para admitir entornos heredados y basados en texto. Este entorno está diseñado con el fin de permitir el uso de un terminal simple o un emulador de terminal.
7. Especifique las siguientes opciones personalizadas para aumentar la compatibilidad con los terminales existentes:
   - Edición de línea
   - Control de eliminación
   - Control del eco
   - Control del protocolo de enlace
   - Nueva secuencia de línea
   - Introducir nueva secuencia de línea
8. Haga clic en **Aplicar cambios**.
9. Haga clic en **Volver a la ventana de configuración del puerto serie** para regresar a la ventana **Configuración del puerto serie**.

Configuración del dispositivo de acceso remoto para usar una comunicación en serie en la LAN

Para configurar BMC/iDRAC para comunicaciones en una conexión LAN (SOL):

1. Haga clic en el objeto **Gabinete modular** > **Módulo del servidor/sistema** > **Chasis del sistema principal/Sistema principal** > **Acceso remoto**.
2. Haga clic en la pestaña **Configuración**.
3. Haga clic en **Comunicación en serie en la LAN**.

   Aparecerá la ventana **Configuración de la comunicación en serie en la LAN**.
4. Configure los siguientes detalles:
   - Activar comunicación en serie en la LAN
   - Velocidad en baudios
   - Privilegio mínimo necesario
5. Haga clic en **Aplicar cambios**.
6. Haga clic en **Configuración avanzada** para definir más opciones de configuración de BMC.
7. En la ventana **Configuración avanzada de la comunicación en serie en la LAN** puede configurar la siguiente información:
   - Intervalo de acumulación de caracteres
   - Umbral de envío de caracteres
8. Haga clic en **Aplicar cambios**.
9. Haga clic en **Volver a la configuración de la comunicación en serie en la LAN** para regresar a la ventana **Configuración de la comunicación en serie en la LAN**.

Configuración adicional para iDRAC

Para configurar las propiedades de IPv4 e IPv6 por medio de la pestaña **Configuración adicional**:

1. Haga clic en **Gabinete modular→ Módulo del servidor/sistema → Chasis del sistema principal/Sistema principal→ Acceso remoto**
2. Haga clic en la pestaña **Configuración**.
3. Haga clic en **Configuración adicional.**
4. Configure las propiedades de IPv4 e IPv6 con el valor **Activado** o **Desactivado**.
5. Haga clic en **Aplicar cambios**.

   NOTA: Para obtener información acerca de la administración de licencias, consulte la *Guía del usuario de Dell License Manager* disponible en `dell.com/openmanagemanuals`.

Configuración de usuarios del dispositivo de acceso remoto

Para configurar los usuarios del dispositivo de acceso remoto mediante la página Acceso remoto:

1. Haga clic en el objeto **Gabinete modular** > **Módulo del servidor/sistema** > **Chasis del sistema principal/Sistema principal** > **Acceso remoto**.
2. Haga clic en la ficha **Usuarios**.

   La ventana **Usuarios de acceso remoto** muestra información acerca de los usuarios que se pueden configurar como usuarios de BMC/iDRAC.
3. Haga clic en **Id. de usuario** para configurar un usuario nuevo o existente de BMC/iDRAC.

   La ventana **Configuración de usuario de acceso remoto** le permite configurar un usuario específico de BMC/iDRAC.
4. Especifique la siguiente información general:
   - Seleccione **Activar el usuario** para activarlo.

- Introduzca el nombre del usuario en el campo **Nombre del usuario**.
- Seleccione la casilla **Cambiar contraseña**.
- Introduzca una nueva contraseña en el campo **Nueva contraseña**.
- Vuelva a escribir la nueva contraseña en el campo **Confirmar contraseña nueva**.

5. Especifique los siguientes privilegios del usuario:
   - Seleccione el límite máximo de nivel de privilegio del usuario de LAN.
   - Seleccione el nivel de privilegio máximo permitido de usuario para el puerto serie.
6. Especifique el grupo de usuarios para los privilegios de usuario de DRAC/iDRAC.
7. Haga clic en **Aplicar cambios** para guardar los cambios.
8. Haga clic en **Volver a la ventana Usuario de acceso remoto** para volver a la ventana **Usuarios de acceso remoto**.

   NOTA: Una vez que DRAC está instalada, se pueden configurar seis entradas de usuario adicionales. Esta acción da como resultado un total de 16 usuarios. Las mismas reglas de nombre de usuario y contraseña se aplican a los usuarios de BMC/iDRAC y RAC. Una vez instalado DRAC/iDRAC6, las 16 entradas de usuario se asignan a DRAC.

Establecimiento de alertas de filtro para eventos de plataforma

Para configurar las funciones más relevantes del BMC, como los parámetros de filtro para sucesos de plataforma (PEF) y destinos de alertas mediante Server Administrator Instrumentation Service:

1. Haga clic en el objeto **Sistema**.
2. Haga clic en la ficha **Administración de alertas.**
3. Haga clic en **Sucesos de plataforma**.

   La ventana **Sucesos de plataforma** le permite realizar acciones individuales en respuesta a determinados sucesos de plataforma. Puede seleccionar los sucesos para los que desee efectuar acciones de apagado y generar alertas para las acciones seleccionadas. Además, puede enviar alertas para destinos con las direcciones IP específicas que elija.

   NOTA: Para configurar las alertas de PEF del BMC, debe haber iniciado sesión con privilegios de administrador.

   NOTA: La configuración **Habilitar alertas de filtros de sucesos de plataforma** deshabilita o habilita la generación de alertas de PEF. Es independiente de la configuración de alertas de sucesos de plataforma individuales.

   NOTA: El **Aviso de sonda de alimentación del sistema** y la **Falla de sonda de la alimentación del sistema** no se admiten en los sistemas PowerEdge incompatibles con PMBus, a pesar de que Server Administrator le permita configurarlos.

4. Elija el suceso de plataforma para el que desea realizar acciones de apagado o generar alertas para acciones seleccionadas, y haga clic en **Establecer sucesos de plataforma**.

   La ventana **Establecer sucesos de plataforma** le permite especificar las acciones que se realizarán en caso de que vaya a apagarse el sistema en respuesta a un suceso de plataforma.

5. Seleccione una de las siguientes acciones:
   - **Ninguno**
   - **Reiniciar sistema**

     Apaga el sistema operativo e inicia el arranque del sistema, realiza comprobaciones del BIOS y recarga el sistema operativo.

   - **Apagar el sistema**

     Apaga la alimentación eléctrica al sistema.

   - **Realizar ciclo de encendido del sistema**

     Apaga la alimentación eléctrica del sistema, realiza una pausa, enciende la alimentación y reinicia el sistema. El ciclo de encendido resulta útil cuando se desean reinicializar componentes del sistema como las unidades de disco duro.

   - **Reducción de alimentación**

     Detiene la CPU.

PRECAUCIÓN: Al configurar una opción diferente a Ninguno o Reducción de la alimentación para una acción de apagado relacionada con un suceso de plataforma, el sistema se ve obligado a apagarse cuando tenga lugar el suceso especificado. El firmware inicia este apagado, que se realiza sin cerrar primero el sistema operativo ni ninguna aplicación que se esté ejecutando.

NOTA: No todos los sistemas admiten la reducción de alimentación. Las funciones Supervisión de fuentes de alimentación y Supervisión de la alimentación solo están disponibles para aquellos sistemas que tengan dos o más suministros de energía redundantes con capacidad de intercambio dinámico instaladas. Estas funciones no están disponibles para aquellos suministros de energía redundantes instalados de forma permanente que no dispongan de circuitería de administración de energía.

6. Seleccione la casilla **Generar alerta** para enviar las alertas.

   NOTA: Para generar una alerta, debe seleccionar las configuraciones **Generar alerta** y **Habilitar alertas de sucesos de plataforma**.

7. Haga clic en **Aplicar**.
8. Haga clic en **Aplicar a la página de sucesos de plataforma** para volver a la ventana **Filtros de sucesos de plataforma**.

Definición de destinos de alerta para eventos de plataforma

También puede utilizar la ventana Filtros de evento de plataforma para seleccionar un destino donde se envíe una alerta de evento de plataforma. Según la cantidad de destinos que se muestren, puede configurar una dirección IP separada para cada dirección de destino. Se envía una alerta de suceso de plataforma a cada dirección IP de destino que se configura.

1. Haga clic en **Configurar destinos** en la ventana Filtros del suceso de plataforma.
2. Haga clic en el número del destino que desea configurar.

   NOTA: La cantidad de destinos que se pueden configurar en un sistema determinado puede variar.

3. Seleccione la casilla **Activar destino**.
4. Haga clic en **Número de destino** para agregar una dirección IP individual para ese destino. Esta es la dirección IP a la que se envía la alerta del evento de plataforma.

   NOTA: En los sistemas de 12º generación con versiones especificas de iDRAC7, puede establecer el destino de sucesos de la plataforma como IPv4, IPv6 o FQDN.

5. Introduzca un valor en el campo **Cadena de comunidad** que funcione como una contraseña para autenticar los mensajes que se envían entre una estación de administración y un sistema administrado. La cadena de comunidad (también llamada "nombre de comunidad") se envía en cada paquete entre la estación de administración y un sistema administrado.
6. Haga clic en **Aplicar**.
7. Haga clic en **Volver a la página de sucesos de plataforma** para volver a la ventana **Filtros del suceso de plataforma**.

7

Configurar acciones de alerta

Temas:

Establecimiento de acciones de alerta para sistemas que ejecutan sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server compatibles

Cuando establece acciones de alerta para un evento, puede especificar que la acción muestre una alerta en el servidor. Para realizar esta acción, Server Administrator envía un mensaje a `/dev/console`. Si el sistema de Server Administrator ejecuta un sistema X Window, el mensaje no se muestra. Para ver el mensaje de alerta en sistemas Red Hat Enterprise Linux mientras se ejecuta el sistema X Window, debe iniciar **xconsole** o **xterm -C** antes de que ocurra el evento. Para ver el mensaje de alerta en sistemas SUSE Linux Enterprise Server mientras se ejecuta el sistema X Window, debe iniciar **xterm -C** antes de que ocurra el evento.

Cuando establece acciones de alerta para un evento, puede especificar la acción para **difundir un mensaje**. Para realizar esta acción, Server Administrator ejecuta el comando wall, que envía el mensaje a todos aquellos usuarios que hayan iniciado sesión con su permiso de mensajes configurado en **sí**. Si el sistema de Server Administrator está ejecutando un sistema X Window, el mensaje no se mostrará de manera predeterminada. Para ver el mensaje de difusión mientras el sistema X Window se está ejecutando, debe iniciar un terminal, como **xterm** o **gnome-terminal**, antes de que ocurra el evento.

Cuando establece acciones de alerta para un evento, puede especificar la acción para **ejecutar la aplicación**. Existen limitaciones en las aplicaciones que Server Administrator puede ejecutar. Para garantizar una ejecución adecuada:

- No especifique aplicaciones basadas en el sistema X Window, ya que Server Administrator no puede ejecutar estas aplicaciones correctamente.
- No especifique aplicaciones que requieran que el usuario introduzca información, ya que Server Administrator no puede ejecutar estas aplicaciones correctamente.
- Redirija **stdout** y **stderr** a un archivo cuando especifique la aplicación, de manera que pueda ver todos los mensajes de salida o error.
- Si desea ejecutar varias aplicaciones (o comandos) para una alerta, cree una secuencia para hacerlo y escriba la ruta de acceso completa en la secuencia en el cuadro **Ruta de acceso absoluta a la aplicación**.

Ejemplo 1: `ps -ef >/tmp/psout.txt 2>&1`

El comando en el ejemplo 1 ejecuta el comando de aplicación ps, redirije stdout al archivo **/tmp/psout.txt** y redirije **stderr** al mismo archivo que **stdout**.

Ejemplo 2: `mail -s "Server Alert" admin </tmp/alertmsg.txt>/tmp/mailout.txt 2>&1`

El comando en el ejemplo 2 ejecuta la aplicación de correo para enviar el mensaje que contiene el archivo `/tmp/alertmsg.txt`al usuario de Red Hat Enterprise Linux o SUSE Linux Enterprise Server y al administrador con el asunto **Alerta de servidor**. El usuario debe crear el archivo `/tmp/alertmsg.txt` antes de que ocurra el evento. Además, **stdout** y **stderr** se redirigen al archivo `/tmp/mailout.txt` en caso de que se produzca un error.

Acciones de alerta de la configuración en Windows Server para ejecutar aplicaciones

En Windows, la **Detección de servicios interactivos** está deshabilitada por defecto. La **Detección de servicios interactivos** debe habilitarse en **Regedit** para habilitar las aplicaciones ejecutables.

Para habilitar **Detección de servicios interactivos** siga los pasos que se mencionan a continuación:

Modifying the **NoInteractiveServices**

1. Abra **Regedit**.
2. Vaya a `HKLM\SYSTEM\CurrentControlSet\Control\Windows\`.
3. Haga clic con el botón derecho en **NoInteractiveServices** y haga clic en **Modificar**.
4. En **Información del valor**, introduzca **0** y haga clic en **Aceptar**.
5. Cierre **Regedit**
6. Para agregar el usuario a un grupo, seleccione el nombre del grupo en el menú desplegable **Grupo** y haga clic en **Agregar**.
7. Haga clic en **Aceptar**.

Enabling the **Interactive Service Detection**

8. Abra **Services.msc**.
9. Vaya a **Detección de servicios interactivos**.
10. Haga clic con el botón derecho en **Detección de servicios interactivos** y seleccione **Propiedades**.
11. En la pestaña **General**, cambie **Tipo de inicio** a **Automático** y haga clic en **Aplicar**.
12. En Estado del servicio, haga clic en **Iniciar**.

Allowing the service to interact

13. Vaya al **Administrador de datos de DSM SA**, haga clic con el botón derecho y, a continuación, haga clic en **Propiedades**.
14. En la pestaña **Iniciar sesión**, habilite la opción **Permitir la interacción del servicio con el escritorio** y haga clic en **Aplicar**.
15. Haga clic en **Aceptar**.

Reinicie el **Administrador de datos de DSM SA** para habilitar la **Detección de servicios interactivos**.

Aplicación interactiva: Algunos ejemplos de aplicaciones interactivas son aplicaciones con una interfaz gráfica de usuario (GUI) o que solicitan al usuario la introducción de información de cierta forma, como el comando "pause" en un archivo de procesamiento en lote.

NOTA: Para ver la aplicación interactiva, aparece un mensaje emergente **Detección de servicios interactivos** con la siguiente información: `A program running on this computer is trying to display a message`, haga clic en **Ver el mensaje** para continuar.

Mensajes de alertas de filtro para eventos de plataforma de BMC/iDRAC

La tabla siguiente especifica todos los mensajes de filtro para eventos de plataforma (PEF) posibles junto con una descripción de cada evento.

Tabla 14. Eventos de alerta de PEF

Suceso	Descripción
Fallo de sonda del ventilador	El ventilador está funcionando muy lentamente o no está funcionando en absoluto.
Fallo de sonda de voltaje	El voltaje es demasiado bajo para una operación adecuada.
Aviso de sonda de baterías	La batería está funcionando por debajo del nivel de carga recomendado.
Error en sonda de baterías	La batería ha fallado.
Fallo de sonda de voltaje discreta	El voltaje es demasiado bajo para una operación adecuada.
Aviso de sonda de temperatura	La temperatura está llegando a un límite excesivamente alto o bajo.
Fallo de sonda de temperatura	La temperatura es demasiado alta o demasiado baja para una operación adecuada.
Intrusión en el chasis detectada	El chasis del sistema se ha abierto.
Redundancia (de suministro de energía o ventilador) degradada	La redundancia para los ventiladores y/o los suministros de energía se ha reducido.
Redundancia (de suministro de energía o ventilador) perdida	No hay redundancia restante para los ventiladores y/o los suministros de energía del sistema.

Tabla 14. Eventos de alerta de PEF

Suceso	Descripción
Aviso del procesador	Un procesador se está ejecutando con un rendimiento o a una velocidad menor al óptimo.
Fallo del procesador	Un procesador ha fallado.
Procesador ausente	Se ha quitado un procesador.
Aviso de PS/VRM/D2D	El suministro de energía, el módulo regulador de voltaje o el convertidor de CC a CC tiene una condición de fallo pendiente.
Error de PS/VRM/D2D	El suministro de energía, el módulo regulador de voltaje o el convertidor de CC a CC ha fallado.
El registro de hardware está lleno o se ha vaciado	Un registro de hardware lleno o vacío requiere la atención del administrador.
Recuperación de sistema automática	El sistema está bloqueado o no responde, y está realizando una acción configurada por la recuperación automática del sistema.
Aviso de sonda de alimentación del sistema	El nivel de consumo de energía se aproxima al umbral de error.
Fallo de sonda de la alimentación del sistema	El nivel de consumo de energía ha superado el máximo límite admisible y ha producido un error.
Medios flash extraíbles ausentes	Se ha quitado la unidad flash extraíble.
Soportes flash extraíbles con error	La unidad flash extraíble tiene una condición de error pendiente.
Aviso de medios flash extraíbles	Los medios flash extraíbles tienen una condición de error pendiente.
Error crítico en la tarjeta del módulo SD dual interno	Se ha producido un error en la tarjeta del módulo SD dual interno.
Aviso en la tarjeta del módulo SD dual interno	La tarjeta del módulo SD dual interno tiene una condición de error pendiente.
Se ha perdido la redundancia de la tarjeta del módulo SD dual interno.	La tarjeta del módulo SD dual interno no tiene redundancia.
Tarjeta del módulo SD dual interno ausente	Se ha quitado la tarjeta del módulo SD dual interno.

8

Solución de problemas

Error del servicio de conexión

En Red Hat Enterprise Linux, cuando se envía el comando `SELinux is set to enforced mode`, el servicio de conexión del Server Administrator de Systems Management (SM SA) no puede iniciarse. Realice uno de los siguientes pasos para iniciar este servicio:

- Configure `SELinux` en modo `Disabled` o `Permissive`.
- Cambie la propiedad `allow_execstack` de SELinux al estado **Activado**. Ejecute el comando siguiente:

  ```
  setsebool allow_execstack on
  ```

- Cambie el contexto de seguridad del servicio de conexión del SM SA. Ejecute el siguiente comando: `chcon -t unconfined_execmem_t /opt/dell/srvadmin/sbin/dsm_om_connsvcd`

Temas:

Escenarios de errores de inicio de sesión

No podrá iniciar sesión en el sistema administrado si:

- Introduce una dirección IP incorrecta o no válida.
- Introduce credenciales incorrectas (nombre de usuario y contraseña).
- El sistema administrado está apagado.
- No es posible acceder al sistema administrado debido a una dirección IP no válida o un error de DNS.
- El sistema administrado cuenta con un certificado que no es confiable y no se ha seleccionado la opción **Ignorar advertencias de certificado** en la página de inicio de sesión.
- Los servicios de Server Administrator no están activados en el sistema VMware ESXi. Para obtener información sobre cómo activar los servicios de Server Administrator en el sistema VMware ESXi, consulte la *Guía de instalación de Server Administrator* en `dell.com/openmanagemanuals`.
- El servicio Small Footprint CIM Broker Daemon (SFCBD) del sistema VMware ESXi no se está ejecutando.
- El servicio de administración de Web Server del sistema administrado no se está ejecutando.
- Se introdujo la dirección IP del sistema administrado sin el nombre del host y no se ha seleccionado la casilla **Ignorar advertencias de certificado**.
- La función Autorización de WinRM (Remote Enablement) no está configurada en el sistema administrado. Para obtener más información sobre esta función, consulte la *Guía de instalación de Server Administrator*, disponible en `dell.com/openmanagemanuals`.
- Se produce un error de autenticación al conectarse con un sistema operativo VMware ESXi 5.0, que puede producirse por cualquiera de los siguientes motivos:
  1. El modo `lockdown` está activado mientras se inicia sesión en el servidor o mientras se está conectado a Server Administrator. Para obtener más información sobre el modo `lockdown`, consulte la documentación de VMware.
  2. La contraseña se cambia mientras se está conectado a Server Administrator.
  3. Inicia sesión en Server Administrator como usuario normal sin privilegios de administrador. Para obtener más información, consulte la documentación de VMware sobre la asignación de la función.

Reparación de una instalación defectuosa de Server Administrator en sistemas operativos Windows admitidos

Para corregir una instalación defectuosa, puede forzar una reinstalación y, a continuación, una desinstalación de Server Administrator.

Para forzar una reinstalación:

1. Compruebe la versión de Server Administrator instalada previamente.
2. Descargue el paquete de instalación para esa versión de **support.dell.com**.
3. Localice `SysMgmt.msi` en el directorio `srvadmin\windows\SystemsManagement`.
4. Escriba el siguiente comando en el símbolo del sistema para forzar la reinstalación

   ```
   msiexec /i SysMgmt.msi REINSTALL=ALL

   REINSTALLMODE=vamus
   ```

5. Seleccione **Configuración personalizada** y elija todas las funciones instaladas originalmente. Si no está seguro de qué funciones se instalaron, selecciónelas todas y efectúe la instalación.

   NOTA: Si instaló Server Administrator en un directorio no predeterminado, asegúrese de cambiarlo también en la **Configuración personalizada**.

   NOTA: Después de instalar la aplicación, puede desinstalar Server Administrator mediante la opción **Agregar o quitar programas**.

Servicios de Server Administrator

La siguiente tabla muestra los servicios que utiliza Server Administrator para proporcionar información sobre la administración de sistemas y el impacto que provoca la presencia de errores en estos servicios.

Tabla 15. Servicios de Server Administrator (continuación)

Nombre del servicio	Descripción	Impacto del error	Mecanismo de recuperación	Gravedad
Windows: servicio de conexión de SM SA Linux: `dsm_om_connsvc` (este servicio se instala con Server Administrator Web Server).	Brinda acceso local/ remoto a Server Administrator desde cualquier sistema con explorador web compatible y conexión de red.	Los usuarios no pueden iniciar sesión en Server Administrator ni pueden realizar ninguna operación a través de la interfaz de usuario web. Sin embargo, aún se puede utilizar la CLI.	Reinicie el servicio	Crítico
Windows: servicios compartidos de SM SA Linux: `dsm_om_shrsvc` (este servicio se ejecuta en el sistema administrado).	Ejecuta el recopilador de inventarios durante el inicio para generar un inventario del software del sistema que utilizan los proveedores de SNMP y CIM de Server Administrator a fin de realizar una actualización remota de software mediante la consola de administración del sistema y Dell OpenManage Essentials.	Las actualizaciones de software no se pueden efectuar mediante OpenManage Essentials. Sin embargo, las actualizaciones aún se pueden realizar de forma local y fuera de Server Administrator mediante Dell Update Packages individuales. Todavía se pueden realizar actualizaciones mediante herramientas de terceros (por ejemplo,	Reinicie el servicio	Aviso

Tabla 15. Servicios de Server Administrator

Nombre del servicio	Descripción	Impacto del error	Mecanismo de recuperación	Gravedad
		MSSMS, Altiris y Novell ZENworks).		
NOTA: Server Administrator puede enviar capturas de SNMP duplicadas o registrar sucesos duplicados en la página Registro de alertas o en el archivo de registro del sistema operativo. Las capturas y los sucesos duplicados se registran cuando los servicios de Server Administrator se reinician manualmente o cuando el sensor del dispositivo aún indica un estado anómalo cuando los servicios de Server Administrator se inician después de un reinicio del sistema operativo. **NOTA:** El recopilador de inventarios es necesario para actualizar las consolas Dell mediante Dell Update Packages. **NOTA:** Algunas de las funciones del recopilador de inventarios no se admiten en Server Administrator (64 bits).				
Windows: administrador de eventos de SM SA Linux: `dsm_sa_datamgrd` (alojado en el servicio dataeng) (este servicio se ejecuta en el sistema administrado).	Supervisa el sistema, ofrece acceso rápido a información detallada sobre errores y rendimiento, y permite la administración remota de sistemas supervisados, incluidos el apagado, el inicio y la seguridad.	Los usuarios no pueden configurar ni ver los detalles de nivel de hardware en la GUI/CLI sin que estos servicios estén en ejecución.	Reinicie el servicio	Crítico
Administrador de eventos de SM SA (Windows) Linux: `dsm_sa_eventmgrd` (alojado en el servicio dataeng) (este servicio se ejecuta en el sistema administrado).	Proporciona el servicio de registro de eventos de archivos y sistema operativo para la administración de sistemas, y también es usado por analizadores de registros de eventos.	Si se detiene este servicio, no funcionan correctamente las funciones de registro de eventos.	Reinicie el servicio	Aviso
Linux: `dsm_sa_snmpd` (alojado en el servicio dataeng) (este servicio se ejecuta en el sistema administrado).	Interfaz del motor de datos SNMP de Linux	La solicitud SNMP para obtener/establecer/capturar no funciona desde una estación de administración.	Reinicie el servicio	Crítico
Windows: `mr2kserv` (este servicio se ejecuta en el sistema administrado).	Storage Management Service brinda información de administración de almacenamiento y funciones avanzadas para configurar un medio de almacenamiento local o remoto conectado al sistema.	El usuario no puede ejecutar funciones de almacenamiento para todas las controladoras RAID y no RAID admitidas.	Reinicie el servicio	Crítico

9

Preguntas frecuentes

En esta sección se enumeran las preguntas más frecuentes acerca de Server Administrator:

NOTA: Las preguntas siguientes no son específicas para esta versión de Server Administrator.

1. **¿Cuál es el nivel de permiso mínimo que se requiere para instalar Server Administrator?**

   Para instalar Server Administrator, debe tener privilegios de nivel de administrador. Los usuarios y los usuarios avanzados no tienen permisos para instalar Server Administrator.
2. **¿Cómo puedo determinar cuál es la versión más reciente de Server Administrator disponible para mi sistema?**

   Acceda a: **dell.com/support** → Software y Seguridad → Enterprise System Management → OpenManage Server Administrator.

   Todas las versiones disponibles de Server Administrator se muestran en la página.
3. **¿Cómo puedo saber cuál es la versión de Server Administrator que se ejecuta en mi sistema?**

   Después de iniciar sesión en Server Administrator, vaya a **Propiedades → Resumen**. Puede encontrar la versión de Server Administrator instalada en el sistema en la columna **Systems Management**.
4. **¿Existen otros puertos que pueden ser utilizados por los usuarios además del puerto 1311?**

   Sí, puede establecer el puerto https preferido. Vaya a **Preferencias → Configuración general → Web Server → Puerto HTTPS**

   En lugar de marcar la opción **Usar predeterminado**, seleccione el botón de radio **Usar** y defina su puerto de preferencia.

   NOTA: Si se cambia el número de puerto a uno no válido o en uso, se puede impedir que otras aplicaciones o exploradores accedan a Server Administrator en el sistema administrado. Para ver la lista de puertos predeterminados, consulte la *Guía de instalación de Server Administrator* disponible en `dell.com/openmanagemanuals`.
5. **¿Puedo instalar Server Administrator en Fedora, College Linux, Mint, Ubuntu, Sabayon o PClinux?**

   No. Server Administrator no admite ninguno de estos sistemas operativos.
6. **¿Server Administrator puede enviar mensajes de correo electrónico si surge un problema?**

   No. Server Administrator no está diseñado para enviar mensajes de correo electrónico cuando surge un problema.
7. **¿Se requiere SNMP para las actualizaciones de software, inventario y descubrimiento por medio de ITA en sistemas PowerEdge? ¿Se puede utilizar CIM por sí solo para el descubrimiento, el inventario y las actualizaciones o se requiere SNMP?**

   ITA *en comunicación con sistemas Linux*:

   En el sistema Linux se requiere SNMP para tareas de descubrimiento, sondeo de estado e inventario.

   Las actualizaciones de software se realizan a través de una sesión SSH y se requieren credenciales/permisos de nivel de raíz y un FTP seguro para ejecutar estas acciones discretas; estos requisitos se solicitan cuando la acción se configura o invoca. No se asumen las credenciales del rango de descubrimiento.

   ITA *en comunicación con sistemas Windows:*

   Para servidores (sistemas que ejecutan sistemas operativos Windows Server), el sistema puede configurarse con SNMP o CIM para descubrimiento por medio de ITA. Para el inventario, se requiere CIM.

   Las actualizaciones de software, como en Linux, no se relacionan con tareas de descubrimiento y sondeo ni con los protocolos utilizados.

   Mediante el uso de las credenciales de nivel de administrador solicitadas en el momento en que se programa o realiza la actualización, se establece un recurso compartido administrativo (unidad) para una unidad del sistema de destino y la copia de archivos desde algún lugar (posiblemente otro recurso compartido de red) se realiza en el sistema de destino. Se invocan las funciones WMI para ejecutar la actualización de software.

   Dado que Server Administrator no se instala en clientes/estaciones de trabajo, se usa el descubrimiento con CIM cuando el sistema de destino ejecuta OpenManage Client Instrumentation.

Para muchos otros dispositivos, como impresoras en red, el estándar es SNMP para comunicarse con el dispositivo (principalmente descubrimiento).

Los dispositivos, como el almacenamiento de EMC, tienen protocolos patentados. Es posible recopilar algunos datos acerca del entorno observando los puertos utilizados.

8. **¿Existen planes referidos a la compatibilidad con SNMP v3?**

   No, no existen planes para la compatibilidad con SNMP v3.

9. **¿El uso de un carácter de guión bajo en el nombre de dominio puede causar problemas de inicio de sesión en Server Administrator?**

   Sí, los caracteres de guion bajo en el nombre de dominio no son válidos. Todos los demás caracteres especiales (excepto el guion) tampoco son válidos. Utilice abecedarios que distingan mayúsculas de minúsculas y numerales solamente.

10. **¿Cuál es el efecto de elegir o no la opción Active Directory en la página de inicio de sesión de Server Administrator en relación con los niveles de privilegio?**

    Si no selecciona la casilla Active Directory, solamente tendrá acceso según lo configurado en Microsoft Active Directory. No puede iniciar sesión con la solución de esquema extendido en Microsoft Active Directory.

    Esta solución permite otorgar acceso a Server Administrator; lo cual permite agregar y controlar usuarios y privilegios de Server Administrator a usuarios existentes en el software de Active Directory. Para obtener más información, consulte "Uso de Microsoft Active Directory" en la *Guía de instalación de Server Administrator* disponible en **dell.com/openmanagemanuals**.

11. **¿Qué acciones debo ejecutar al realizar la autentificación con Kerberos e intentar iniciar sesión desde Web Server?**

    Para la autentificación, se debe reemplazar el contenido de los archivos **/etc/pam.d/openwsman** y **/etc/pam.d/sfcb**, en el nodo administrado:

    ```
    auth required pam_stack.so service=system-auth auth required /lib64/security/pam_nologin.so
    account required pam_stack.so service=system-auth
    ```

12. **Las alertas de Server Administrator no se muestran en una captura SNMP, ¿cómo se puede cambiar la configuración para activar las capturas SNMP?**

    Siga los pasos para cambiar la configuración de SNMP para activar las alertas de Server Administrator:

    - `esxcli system snmp set --communities public`
    - `esxcli network firewall ruleset set --ruleset-id snmp --allowed-all true`
    - `esxcli network firewall ruleset set --ruleset-id snmp --enabled true`
    - `esxcli system snmp set -t <target_ip>@162/public`
    - `esxcli system snmp set --enable true`