Dell OpenManage Server Administrator versión 7.4

Guía del usuario

Notas, precauciones y avisos

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.

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

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

2014 - 03

Rev. A00

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 al proporcionar una solución de 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 de sistemas locales y remotos fácil de usar 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).

Instalación

Puede instalar Server Administrator mediante *Dell Systems Management Tools and Documentation DVD (DVD de herramientas y documentación de Dell Systems Management)*. El DVD proporciona un programa de configuración para instalar, actualizar y desinstalar Server Administrator, y los componentes de software de la estación de administración y del sistema administrado. Además, puede instalar Server Administrator en varios sistemas mediante una instalación desatendida a través de una red. El instalador de Server Administrator proporciona secuencias de instalación y paquetes RPM para instalar y desinstalar Server Administrator y otros componentes de software del sistema administrado. Para obtener más información, consulte la *Server Administrator Installation Guide (Guía de instalación de Server Administrator)* y la *Management Station Software Installation Guide (Guía de instalación del software Management Station)* en **dell.com/openmanagemanuals**.

NOTA: Cuando instala los paquetes de código abierto desde *Dell Systems Management Tools and Documentation DVD (DVD de herramientas y documentación de Dell Systems Management)*, los archivos de licencia se copian automáticamente en el sistema. Al eliminar estos paquetes, los archivos de licencia correspondientes también se eliminan.

NOTA: Si tiene un sistema modular, debe instalar Server Administrator en cada uno de los módulos del servidor instalados en el chasis.

Actualización de los componentes individuales del sistema

Para actualizar componentes individuales del sistema, utilice Dell Update Packages específicos de los componentes. Use *Dell Server Update Utility DVD (DVD de Dell Server Update Utility)* para ver el informe completo de la versión y actualizar un sistema entero. Server Update Utility (SUU) se puede descargar también de **dell.com/support.**

NOTA: Para obtener más información sobre cómo obtener y usar Server Update Utility (SUU), para actualizar sistemas Dell o par ver las actualizaciones disponibles de cualquier sistema que se muestre en el repositorio, consulte la *Dell Server Update Utility User's Guide (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 *Server Administrator Storage Management* en **dell.com/openmanagemanuals**.

Instrumentation Service

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

Remote Access Controller

Remote Access Controller ofrece una solución completa de administración del sistema remota para sistemas equipados con Dell Remote Access Controller (DRAC) o la solución de controladora 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, permitiéndole poner el sistema en funcionamiento lo más rápido posible. Remote Access Controller también proporciona 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 los bloqueos del sistema y guarda la pantalla de bloqueo más reciente.

Registros

Server Administrator muestra registros de comandos emitidos al sistema (o bien, por el sistema), sucesos de hardware supervisados, sucesos POST 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.

Novedades de esta versión

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

- Se agregó compatibilidad con los siguientes sistemas operativos:
  - Microsoft Windows Server 2012 R2 Datacenter, Foundation, Essentials, y Standard Edition
  - Novell SUSE Linux Enterprise Server 11 SP3 (64 bits)
  - Red Hat Enterprise Linux 6.5 (64 bits)
  - VMware ESXi 5.0 U3 y ESXi 5.1 U2
  - VMware vSphere 5.5
- Compatibilidad agregada para los siguientes exploradores:
  - Mozilla Firefox 22 y 23
  - Internet Explorer 11
  - Safari 6.0
  - Google Chrome 27, 28 y 30
- Compatibilidad para un nuevo formato de la licencia para Citrix XenServer 6.1
- Compatibilidad agregada para las siguientes tarjetas de adaptador:
  - Adaptador de red Mellanox ConnectX-3 Dual Port 40 GbE QSFP+
  - Adaptador de red Mellanox ConnectX-3 Dual Port 10 GbE DA/SFP+
  - Tarjeta Mezzanine Mellanox ConnectX-3 Dual Port 10 GbE KR Blade
  - Emulex OCe14102-UX-D Dual Port 10 Gb SFP+ CNA
  - Emulex OCm14102-U3-D Dual Port 10 Gb KR Blade Mezz
  - Emulex OCm14102-U2-D Dual Port 10 Gb KR Blade NDC
  - Emulex OCm14104-UX-D Quad Port 10 Gb DA/SFP+ Rack NDC
- Compatibilidad para mostrar y establecer la versión de JRE. Consulte Sistema de puerto seguro.
- Compatibilidad para mostrar la identificación de nodo en la información de resumen del módulo del sistema o servidor. Consulte la *Guía de la interfaz de línea de comandos de Server Administrator* o la ayuda en línea.
- Compatibilidad para nuevos valores para la alineación del factor de forma con los valores del iDRAC. Consulte la *Guía de la interfaz de línea de comandos de Server Administrator* o la ayuda en línea.
- Se agregó compatibilidad para las controladoras RAID de software (PERC S110) en sistemas que ejecutan el sistema operativo de Windows Server 2012 R2.
- Se agregó compatibilidad para las unidades de estado sólido de memoria no volátil Express (NVMe) de Interconexión de componentes periféricos Express (PCIe). Consulte la guía de *Server Administrator Storage Management* en **dell.com/openmanagemanuals**.

  NOTA: La administración de dispositivos Dell PowerEdge Express Flash NVMe PCIe SSD sólo se admite a través de los controladores de Windows Server 2012 R2 (64 bits) proporcionados por Dell.
- Se agregó compatibilidad para las controladoras Dell PERC 9 (adaptador H730P) en R920 con las siguientes funciones:
  - Disco virtual RAID 10 con tramo irregular.

  - Unidades de disco duro avanzadas de sector de 4 KB.
  - Información de protección (PI) T10 para la integridad de los datos.

    NOTA: Para obtener más información, consulte la guía de *Server Administrator Storage Management* en dell.com/openmanagemanuals.
- Se agregó compatibilidad para los siguientes Adaptadores de bus host (HBA) SAS LSI Serial Attached SCSI en los sistemas de 12 ° generación admitidos:
  - SAS LSI 9207-8e
  - SAS LSI 9300-8e
  - SAS LSI 9206-16e
- Se agregó compatibilidad para los siguientes servidores Dell PowerEdge:
  - R920
  - R220
  - M820VRTX
- Ya no se brinda compatibilidad con los siguientes sistemas operativos:
  - SUSE Linux Enterprise Server 10 SP4
  - SUSE Linux Enterprise Server 11 SP2
  - Red Hat Enterprise Linux 6.4 (64 bits)
  - VMware ESXi 5.1 U1 HDD y Flash
  - VMware ESXi 5.0 U2 HDD y Flash

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

NOTA: Para obtener más información sobre las funciones que se introdujeron en esta versión, consulte la ayuda contextual en línea de Server Administrator.

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 el sistema admite SNMP, debe instalar y activar 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 algunos casos, de la versión del sistema operativo.

NOTA: Para obtener información sobre cuestiones de seguridad de SNMP, consulte el archivo Léame de Server Administrator (incluido en la aplicación de Server Administrator) o en **dell.com/openmanagemanuals**. Debe aplicar las actualizaciones de los agentes SNMP maestros del sistema operativo para garantizar la seguridad de los subagentes SNMP de Dell.

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 OpenManage Essentials mientras se está conectado 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 2008 y familia Windows Server 2003	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 ESX	Disponible en el paquete net-snmp instalado por el sistema operativo	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
Citrix XenServer 6.0	Disponible en el paquete net-snmp desde el medio de instalación del sistema operativo	No disponible

Página principal de Server Administrator

La página de inicio de **Server Administrator** ofrece tareas de administración de sistema basadas en exploradores web de fácil configuración y uso desde el sistema administrado o un host remoto a través

de una red LAN, un servicio dial-up o una red inalámbrica. Cuando el servicio de conexión de Dell Systems Management Server Administrator (servicio de conexión de DSM SA) está instalado y configurado en el sistema administrado, es posible ejecutar funciones de administración remota desde cualquier sistema que cuente con un explorador web y una conexión compatibles. De manera adicional, la página de inicio de Server Administrator ofrece ayuda en línea contextual extendida.

Otros documentos que podrían ser de utilidad

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

- *Dell Systems Software Support Matrix (Matriz de compatibilidad de software de los sistemas Dell)* ofrece información sobre los diversos sistemas Dell, los sistemas operativos compatibles con esos sistemas y los componentes que se pueden instalar en estos sistemas.
- En la *Guía de instalación de Server Administrator* se incluyen instrucciones para ayudar a instalar Dell OpenManage Server Administrator.
- La *Management Station Software Installation Guide (Guía de instalación del software Management Station)* contiene instrucciones para ayudarlo a instalar el software Dell OpenManage Management Station.
- La *OpenManage SNMP Reference Guide (Guía de referencia de SNMP de OpenManage)* documenta la base de información de administración (MIB) del protocolo simple de administración de red (SNMP).
- En *Dell OpenManage Server Administrator CIM Reference Guide (Guía de referencia del CIM de Dell OpenManage Server Administrator)*, se describe el proveedor del modelo común de información (CIM), una extensión del archivo de formato de objeto de administración (MOF) estándar.
- En *Messages Reference Guide (Guía de referencia de mensajes)* se presenta una lista de los mensajes que aparecen en el registro de alertas de la página de inicio de Server Administrator o en el visor de sucesos del sistema operativo.
- La*Guía de la interfaz de línea de comandos de Server Administrator* documenta la interfaz de línea de comandos completa de Server Administrator.
- La *Guía del usuario de Dell Remote Access Controller 5* proporciona información completa acerca del uso de la utilidad de línea de comandos RACADM para configurar un DRAC 5.
- La *Guía del usuario de Dell Chassis Management Controller* proporciona información completa sobre el uso del controlador que administra todos los módulos en el chasis que contiene el sistema Dell.
- La *Guía de referencia de línea de comandos para iDRAC6 y CMC* proporciona información acerca de subcomandos RACADM, interfaces compatibles, grupos de bases de datos de propiedad y definiciones de objeto para iDRAC6 y 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 12° 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 11° 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° generación a fin de administrar y supervisar el sistema y sus recursos compartidos de forma remota a través de una red.
- *Dell Online Diagnostics User's Guide (Guía del usuario de Dell Online Diagnostics)* contiene información completa sobre cómo instalar y usar Online Diagnostics en el sistema.
- *Dell OpenManage Baseboard Management Controller Utilities User's Guide (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.

- *Dell OpenManage Server Administrator Storage Management User's Guide (Guía del usuario de Dell OpenManage Server Administrator Storage Management)* es una guía de referencia para la configuración y administración del almacenamiento local y remoto conectado a un sistema.
- *Dell Remote Access Controller Racadm User's Guide (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 de usuario de Dell Remote Access Controller 5* proporciona información completa sobre cómo instalar y configurar una controladora DRAC 5, y cómo usarlo para acceder de manera remota a un sistema que no funciona.
- *Dell Update Packages User's Guide (Guía del usuario de Dell Update Packages)* proporciona información sobre la forma de obtener y usar Dell Update Packages como parte de la estrategia de actualización del sistema.
- *Dell OpenManage Server Update Utility User's Guide (Guía del usuario de Dell OpenManage Server Update Utility)* proporciona información acerca de la obtención y el uso de Server Update Utility (SUU) para actualizar los sistemas Dell o para ver las actualizaciones disponibles para cualquier sistema que aparezca en el repositorio.
- *Dell Management Console User's Guide (Guía del usuario de Dell Management Console)* ofrece información para instalar, configurar y utilizar la consola.
- *Dell Lifecycle Controller User Guide (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.
- *Dell License Manager User's Guide (Guía del usuario de Dell License Manager)* proporciona información sobre cómo administrar licencias de servidor de componentes para los servidores Dell de 12° generación.
- El *Glosario* de términos utilizados en este documento.

Acceso a documentos desde el sitio de asistencia de Dell

Puede acceder a los documentos necesarios en una de las siguientes formas:

- Desde los siguientes enlaces:
  - Para todos los documentos de Systems Management: **dell.com/softwaresecuritymanuals**
  - Para documentos de Enterprise System Management: **dell.com/openmanagemanuals**
  - Para documentos de Remote Enterprise System Management: **dell.com/esmmanuals**
  - Para documentos de Herramientas de servicio: **dell.com/serviceabilitytools**
  - Para documentos de Client Systems Management: **dell.com/OMConnectionsClient**
  - Para documentos de OpenManage Connections Enterprise Systems Management: **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Para documentos de OpenManage Connections Client Systems Management: **dell.com/OMConnectionsClient**
- Desde el sitio de asistencia de Dell de la siguiente manera:
  - Vaya a **dell.com/support/manuals**.
  - En la sección **Información sobre su sistema Dell**, en **No**, seleccione **Elegir de una lista de todos los productos Dell** y haga clic en **Continuar**.
  - En la sección **Seleccione su tipo de producto**, haga clic en **Software y seguridad**.
  - En la sección **Elija su software Dell**, haga clic en el vínculo requerido que corresponda:
    * **Client System Management**
    * **Enterprise System Management**

    * **Remote Enterprise System Management**
    * **Herramientas de servicio**
  – Para ver el documento, haga clic en la versión del producto requerida.
- Uso de los motores de búsqueda de la siguiente manera:
  – 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 asistirlo. Para obtener más información sobre estas herramientas de ayuda, consulte **Getting Help (Cómo obtener ayuda)** en *Hardware Owner's Manual (Manual del propietario de hardware)* del sistema.

Además, está disponible la capacitación y certificación de Dell Enterprise; consulte dell.com/training para obtener más información. Es posible que este servicio no esté disponible en todas las ubicaciones.

Cómo ponerse en contacto con Dell

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

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

1. Vaya a **dell.com/contactdell**.
2. Compruebe su país o región del menú desplegable que hay la esquina superior izquierda de la página.
3. Seleccione su categoría de asistencia: **servicio de asistencia técnica**, **servicio al cliente**, **ventas** o **servicios de soporte internacional**.
4. Seleccione el enlace de servicio o asistencia apropiado de acuerdo a sus requisitos.

NOTA: Si ha comprado un sistema Dell, puede que se le pida la Etiqueta de servicio.

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.

Control de acceso basado en funciones

El control de acceso basado en funciones (RBAC) administra la seguridad al determinar las operaciones que pueden ejecutar los usuarios con funciones específicas. A todos los usuarios se les 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 casi a la estructura de una 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 advertencia y configurar las acciones de alerta que se deberán realizar en caso de advertencia 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, sucesos y comandos. Además, 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

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

Autentificación

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 asegura 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.

Autentificación 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 usando protocolos de administración de cuentas diferentes, como LDAP, NIS, Kerberos y Winbind.

Autenticación de VMware ESX Server 4.X

VMware ESX Server utiliza la estructura de módulos de autenticación conectables (PAM) para la autenticación cuando los usuarios obtienen acceso al host de ESX Server. La configuración de PAM de

los servicios de VMware almacena las rutas de acceso a los módulos de autenticación y se ubica en **/etc/pam.d/vmware-authd**.

La instalación predeterminada de ESX Server utiliza la autentificación **/etc/passwd**, de la misma forma que Linux, aunque ESX Server puede configurarse de tal modo que pueda usar otro mecanismo de autentificación distribuida.

NOTA: En los sistemas que ejecutan el sistema operativo VMware ESX Server 4.x, para iniciar sesión en Server Administrator, todos los usuarios requieren privilegios de administrador. Para obtener más información sobre cómo asignar funciones, consulte la documentación de VMware.

Autenticación de VMware ESXi Server 5.X

ESXi Server autentica los usuarios que acceden a los hosts ESXi con el cliente vSphere/VI o el kit de desarrollo de software (SDK). La instalación predeterminada de ESXi utiliza una base de datos local con contraseña para la autenticación. Las transacciones de autenticación de ESXi con Server Administrator son también interacciones directas con el proceso **vmware-hostd**. Para garantizar la eficacia de la autenticación en el sitio, realice tareas básicas como la configuración de usuarios, grupos, permisos y funciones, al configurar atributos de usuarios, agregar sus propios certificados y determinar si desea utilizar SSL.

NOTA: En sistemas que ejecutan el sistema operativo VMware ESXi Server 5.0, para iniciar sesión en Server Administrator, todos los usuarios deben contar con privilegios de administrador. Para obtener información sobre la asignación de funciones, consulte la documentación de VMware.

Cifrado

El acceso a Server Administrator se realiza mediante una conexión HTTPS segura usando la 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, asigne privilegios de usuario a todos los usuarios del software Dell OpenManage antes de instalar dicho software.

PRECAUCIÓN: Para proteger el acceso a los componentes críticos del sistema, asigne una contraseña a cada cuenta de usuario que pueda acceder al software Dell OpenManage. Los usuarios sin una contraseña asignada no pueden conectarse al software Dell OpenManage en sistemas que ejecuten Windows Server 2003 debido al diseño del sistema operativo.

PRECAUCIÓN: Desactive las cuentas de invitados de los sistemas operativos Windows a fin de proteger el acceso a los componentes críticos del sistema. Cambie el nombre de las cuentas de invitados de modo tal que las secuencias de comandos remotas no puedan activar las cuentas con los nombres de cuentas de invitados predeterminadas.

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 tiene que crear nuevos usuarios desde el software OpenManage.

Cómo agregar usuarios a un dominio en los sistemas operativos Windows

NOTA: Debe tener Microsoft Active Directory instalado en el sistema para realizar los siguientes procedimientos. Consulte Uso del inicio de sesión de Active Directory para obtener más información acerca del 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 mouse en **Usuarios** o haga clic con el botón derecho del mouse 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 en **Terminar**.
5. Haga doble clic en el icono que representa al usuario que acaba de crear.
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.

   Los usuarios nuevos pueden iniciar sesión en el software Dell 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 crear usuarios con privilegios de usuario o usuario avanzado, realice los siguientes pasos.

NOTA: Para realizar los siguientes procedimientos, debe iniciar sesión como `root` o con un nivel de usuario equivalente.

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

Creación de usuarios

NOTA: Para obtener información sobre cómo crear usuarios y grupos de usuarios, consulte la documentación del sistema operativo.

Creación de usuarios con privilegios de usuario

1. Ejecute el siguiente comando en la línea de comandos: `useradd -d <inicio-directorio> -g <grupo> <nombre de usuario>` donde `<grupo>` no es `root`.

   NOTA: Si no existe el `<grupo>`, debe crearlo por medio del comando **groupadd**.
2. Escriba `passwd <nombre de usuario>` y presione <Intro>.

3. Cuando se le solicite, introduzca una 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 <inicio-directorio> -g <grupo> <nombre de usuario>`

   NOTA: Establezca `root` como el grupo principal.
2. Escriba `passwd <nombre de usuario>` y presione <Intro>.
3. Cuando se le solicite, introduzca una 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: Para realizar los siguientes procedimientos, debe iniciar sesión como root o con un nivel de usuario equivalente.

1. Abra el archivo **omarolemap** que se encuentra 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 funciones al archivo `omarolemap`

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

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

   La siguiente tabla enumera ejemplos para agregar la definición de funciones 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
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 el archivo omarolemap:

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

  root * Administrator

  +root * Poweruser

  * * User

- No cambie los permisos de archivo ni el formato del archivo **omarolemap**.
- No utilice la dirección de bucle cerrado para `<nombre del host>`, 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 *nombre de grupo* 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 <*nombre del host*>
- También puede utilizar el `espacio` como delimitador de columnas en lugar de `[Tab]`.

Creación de usuarios de Server Administrator para VMware ESX 4.X, ESXi 4.X y ESXi 5.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 identificación de usuario numérica (UID) y la contraseña, especificando que el nombre de usuario y la UID son opcionales. Si no especifica la UID, vSphere Client asignará la siguiente UID disponible.
5. Para permitir a un usuario el acceso al host ESX/ESXi a través de una shell de comandos, seleccione **Otorgar acceso de shell a este usuario**. Los usuarios que tienen acceso al host solamente mediante vSphere Client 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: Para realizar este procedimiento, debe estar conectado 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 red (SNMP), un estándar de administración de sistemas, en todos los sistemas operativos admitidos. La compatibilidad con SNMP puede o no estar instalada, según el sistema operativo y el modo en que se instaló dicho sistema. En la mayoría de los casos, SNMP se instala como parte de la instalación del sistema operativo. Antes de instalar Server Administrator, se requiere un estándar de protocolo de administración de sistemas admitido, como SNMP.

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 Dell OpenManage Essentials, realice los procedimientos descritos en las siguientes secciones.

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

NOTA: Para que IT Assistant pueda recuperar la información de administración de un sistema que ejecuta Server Administrator, el nombre de comunidad utilizado por IT Assistant debe coincidir con un nombre de comunidad del sistema operativo que ejecuta Server Administrator. Para que IT Assistant modifique la información o realice acciones en un sistema que ejecuta Server Administrator, el nombre de la comunidad utilizado por IT Assistant debe coincidir con un nombre de comunidad que permita operaciones Set en el sistema que ejecuta Server Administrator. Para que IT Assistant recupere capturas (notificaciones de sucesos 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 IT Assistant.

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 ESX 4.X admitidos para MIB VMware Proxy
- Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESXi 4.X y ESXi 5.X admitidos

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 estaciones de administración. Para configurar el agente SNMP para una interacción adecuada con las aplicaciones de administración, como IT Assistant, 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.

Activación del acceso a SNMP en hosts remotos (Windows Server 2003 únicamente)

De forma predeterminada, Windows Server 2003 no acepta paquetes de SNMP desde hosts remotos. Para sistemas que ejecutan Windows Server 2003, debe configurar el servicio SNMP para aceptar paquetes de SNMP desde hosts remotos si planea administrar el sistema mediante aplicaciones de administración de SNMP desde hosts remotos.

Para activar un sistema que ejecuta el sistema operativo Windows Server 2003 para que reciba paquetes de SNMP desde un host remoto:

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**.

   Aparecerá la ventana **Propiedades del servicio SNMP**.
5. Haga clic en la ficha **Seguridad**.
6. Seleccione **Aceptar paquetes de SNMP de cualquier host** o agregue el host remoto a la lista **Aceptar paquetes de SNMP de estos hosts**.

Cambio del nombre de comunidad SNMP

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**.

   Aparecerá 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**.

      Aparecerá 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**.

      Aparecerá 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**.

      Aparecerá 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 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**.

   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 ubica 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 desplegable **Nombre de comunidad** y haga clic en **Agregar** en el cuadro **Destinos de capturas**.

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

   c. En el **Nombre del host**, **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. Es posible configurar el agente SNMP para: cambiar el nombre de la comunidad, activar operaciones Set y enviar capturas a estaciones de administración. Para configurar el agente SNMP para una interacción adecuada con las aplicaciones de administración, como IT Assistant, 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

La identificación 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 los sistemas operativos Red Hat Enterprise Linux y VMware ESXi 4.0, la configuración predeterminada del agente SNMP otorga acceso de solo lectura para la comunidad *public* únicamente para la rama del *sistema* de MIB-II (identificada por la OID 1.3.6.1.2.1.1) del árbol de MIB. Esta configuración no permite que las aplicaciones de administración recuperen o cambien la información de administración de Server Administrator o de otros sistemas fuera de la rama del *sistema* de 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/snm, p/snmpd.conf** de la siguiente forma:

- Crea una vista del árbol de MIB completo al agregar la siguiente línea (si es que 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 es que no existe):

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Cambio del nombre de comunidad SNMP

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.
Para cambiar el nombre de comunidad SNMP con el fin de recuperar 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: Para IPv6, busque la línea `com2sec6 notConfigUser default public`. Asimismo, agregue el texto `agentaddress udp6:161` en el archivo.
3. Edite esta línea reemplazando `public` por el nombre de comunidad SNMP nuevo. Una vez editada, la línea nueva debe aparecer como: `com2sec publicsec default community_name` o `com2sec notConfigUser default community_name`.
4. Para activar los cambios de configuración de SNMP, reinicie el agente SNMP. Para eso, escriba: `service snmpd restart`.

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 que las capturas SNMP se envíen 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 siguientes pasos:

1. Agregue la siguiente línea 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 de configuración de SNMP, reinicie el agente SNMP. Para eso, escriba: `service snmpd restart`.

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

Server Administrator usa los servicios SNMP provistos por el agente net-snmp. Es posible 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 una adecuada interacción con aplicaciones de administración, como IT Assistant, 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 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 es que 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 base de información de administración (MIB) para la comunidad public desde el host local solamente. Esta configuración no permite aplicaciones de administración de SNMP, como IT Assistant, que se ejecuta en otros hosts para descubrir y administrar correctamente 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 a 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 línea nueva debe decir: `rocommunity public IP_address`.

   NOTA: Puede activar el acceso a SNMP desde varios hosts remotos específicos, agregando una directiva `rocommunity` para cada host remoto.
3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo: `/etc/init.d/snmpd restart`.

   Para activar el acceso a SNMP desde todos los hosts remotos a un sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP, **/etc/snmp/snmpd.conf** y realice los siguientes pasos:
4. Busque la línea que dice: `rocommunity public 127.0.0.1`.

5. Edite esta línea borrando 127.0.0.1. Una vez editada, la nueva línea debe decir: `rocommunity public`.
6. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo: `/etc/init.d/snmpd restart`.

Cambio del nombre de comunidad SNMP

Al configurar el nombre de comunidad SNMP, se determinan qué estaciones de administración pueden administrar el sistema mediante SNMP. El nombre de comunidad SNMP utilizado por las aplicaciones de administración debe coincidir con el nombre de comunidad SNMP configurado en el sistema que ejecuta Server Administrator, para que las aplicaciones de administración puedan recuperar la información de administración desde Server Administrator.

Para cambiar el nombre de comunidad SNMP predeterminado utilizado para recuperar la información de administración desde 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. Para editar esta línea, reemplace `public` con el nuevo nombre de comunidad SNMP. Cuando haya finalizado la edición, la nueva línea debería decir: `rocommunity nombre_de_la_comunidad 127.0.0.1.`
4. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo: **/etc/init.d/snmpd restart**.

Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESX 4.X admitidos para MIB VMware Proxy

Es posible administrar el servidor ESX 4.X mediante un único puerto predeterminado 162 con el protocolo SNMP. Para ello, se debe configurar `snmpd` para que utilice el puerto predeterminado 162 y configurar `vmwarehostd` para que utilice un puerto (nuevo) diferente, por ejemplo, 167. Todas las solicitudes de SNMP en la rama de MIB de VMware se redistribuyen a **vmware-hostd** con la función de proxy del daemon de **snmpd**.

Es posible modificar el archivo de configuración de SNMP para VMWware de forma manual en el servidor ESX, o bien, mediante la ejecución del comando de la interfaz de línea de comando remota (RCLI) de VMware, `vicfg-snmp`, desde un sistema remoto (Windows o Linux). Se pueden descargar las herramientas de RCLI desde el sitio web de VMware en **vmware.com/download/vi/drivers_tools.html.**

Para configurar el agente SNMP:

1. Edite el archivo de configuración de SNMP para VMWware, **/etc/vmware/snmp.xml**, de forma manual o mediante la ejecución de los siguientes comandos `vicfg-snmp` para modificar los valores de configuración de SNMP. Esto incluye el puerto de escucha de SNMP, la cadena de comunidad, el puerto o la dirección IP de destino de captura, y el nombre de la comunidad de captura y, a continuación, active el servicio de SNMP para VMware.
   a. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -c <community name> -p X –t <Destination_IP_Address> @162/ <community name>`

      donde: representa un puerto sin usar. Para encontrar un puerto sin usar, compruebe el archivo **/etc/services** de la asignación de puertos para conocer los servicios de sistemas definidos. Además, para asegurarse de que ninguna aplicación o ningún servicio esté actualmente utilizando el puerto seleccionado, ejecute el siguiente comando en el servidor ESX: `netstat –a command`

      NOTA: Pueden ingresarse varias direcciones IP separadas por una coma.

      Para activar el servicio SNMP de VMWare, ejecute el siguiente comando:
   b. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> - E`

      Si desea ver los valores de configuración, ejecute el siguiente comando:
   c. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -s`

      El siguiente es un ejemplo del archivo de configuración, después de haber sido modificado:

```
<?xml version="1.0">

<config>

<snmpSettings>

<enable> true </enable>

<communities> public </communities>

<targets> 143.166.152.248@162/public </targets>

<port> 167 </port>

</snmpSettings>

</config>
```

2. Detenga el servicio SNMP si ya está ejecutándose en el sistema con el siguiente comando: `service snmpd stop`
3. Agregue la siguiente línea al final del archivo **/etc/snmp/snmpd.conf**: `proxy -v 1 -c public udp:127.0.0.1:X .1.3.6.1.4.1.6876`

   Donde `X` representa el puerto no utilizado que se especificó anteriormente durante la configuración de SNMP.

4. Configure el destino de captura con el siguiente comando: `<Destination_IP_Address> <community_name>`

   Se requiere la especificación de trapsink para enviar capturas definidas en las MIB patentadas.
5. Reinicie el servicio mgmt-vmware con el siguiente comando: `service mgmt-vmware restart`
6. Reinicie el servicio snmpd con el siguiente comando: `service snmpd start`

   NOTA: Si srvadmin está instalado y los servicios ya se iniciaron, reinicie los servicios que dependen del servicio **snmpd**.
7. Ejecute el siguiente comando para que el daemon de snmpd se abra con cada reinicio: `chkconfig snmpd on`
8. Ejecute el siguiente comando para asegurarse de que los puertos SNMP estén abiertos antes de enviar capturas a la estación de administración: `esxcfg-firewall -e snmpd`.

Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESXi 4.X y ESXi 5.X admitidos

Server Administrator admite capturas SNMP en VMware ESXi 4.X y ESXi 5.X. Si una licencia independiente está solamente presente, la configuración de SNMP producirá un error en los sistemas operativos VMware ESXi. Server Administrator no admite operaciones Get y Set de SNMP en VMWare ESXi 4.X y ESXi 5.X ya que la compatibilidad de SNMP necesaria no está disponible. La interfaz de línea de comandos (CLI) de VMware vSphere se utiliza para configurar sistemas que ejecutan VMware ESXi 4.X y ESXi 5.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 que las capturas SNMP se envíen 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 para el directorio donde la CLI de VMware vSphere CLI esté instalada. La ubicación predeterminada en Linux es **/usr/bin**. La ubicación predeterminada en Windows es **C:\Archivos de programa\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 nombre de host o la dirección IP del sistema ESXi, `<username>` es un usuario en el sistema ESXi, `<community>` es el nombre de comunidad SNMP y `<hostname>` es el nombre de host 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 que lo haga.

La configuración de capturas SNMP surte efecto inmediatamente, sin reiniciar los servicios.

Configuración del servidor de seguridad en sistemas que ejecutan sistemas operativos compatibles Red Hat Enterprise Linux y SUSE Linux Enterprise Server

Si activa la seguridad del servidor de seguridad mientras instala Red Hat Enterprise Linux o SUSE Linux, el puerto de SNMP se cierra de forma predeterminada en todas las interfaces de red externas. Para permitir que las aplicaciones de administración de SNMP, como IT Assistant, descubran y recuperen la información en Server Administrator, el puerto de SNMP debe estar abierto en al menos una interfaz de red externa. Si Server Administrator detecta que el puerto de SNMP no está abierto en el servidor de seguridad de ninguna interfaz de red externa, Server Administrator muestra un mensaje de advertencia y registra un mensaje en el registro del sistema.

Para abrir el puerto de SNMP, desactive el servidor de seguridad, abra una interfaz de red externa completa en el servidor de seguridad, o bien, abra el puerto de SNMP para al menos una interfaz de red externa en el servidor de seguridad. Puede realizar esta acción antes o después de iniciar Server Administrator.

Para abrir el puerto de SNMP en Red Hat Enterprise Linux utilizando 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.

   Aparece el menú **Elegir una herramienta**.
2. Seleccione **Configuración del servidor de seguridad** utilizando la flecha hacia abajo y presione <Intro>.

   Aparece la pantalla **Configuración del servidor de seguridad**.
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 mediante un asterisco.

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

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

   Aparece la pantalla **Configuración del servidor de seguridad: Personalizar**.
5. Seleccione si desea abrir una interfaz de red completa o solo el puerto de 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 de 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, a continuación, presione **<Intro>**.
   Aparece la pantalla **Configuración del servidor de seguridad**.
7. Presione **<Tab>** para seleccionar **Aceptar** y, a continuación, presione **<Intro>**.
   Aparece el menú **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 ejecutando el 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 <Alt><O> <Alt><N> para ir a la pantalla siguiente.
7. Presione <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 **Iniciar sesión en Server Administrator**. El puerto predeterminado para Server Administrator es 1311. Si es necesario, puede cambiar el puerto. Para obtener instrucciones sobre cómo configurar las preferencias del sistema, consulte Administración de servidores de Dell Systems Management.

NOTA: Los servidores que se ejecutan en XenServer 6.0 se pueden administrar utilizando la interfaz de línea de comandos (CLI) o un servidor de web central instalado en una máquina diferente.

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

Esta forma de inicio de sesión solo se encuentra disponible si los componentes Server Instrumentation y Web Server de Server Administrator están instalados en el sistema local.

Esta opción no está disponible para servidores que se ejecuten en XenServer 6.0.

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 utilizando Microsoft Active Directory. Consulte Uso del inicio de sesión de Active Directory.
3. Haga clic en **Submit (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 *Management Station Software Installation Guide (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

Este inicio de sesión solamente está disponible si el componente Web Server está instalado en el sistema. Para iniciar sesión en Server Administrator con el fin de 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 proporcionado el nombre del sistema o el FQDN, el host de Web Server de Server Administrator convierte el nombre del sistema o el FQDN a la dirección IP del sistema administrado. También puede conectarse si proporciona el número de puerto del sistema administrado en el siguiente formato: nombre de host:número de puerto o dirección IP:número de puerto. Si se conecta a Citrix XenServer, Server Administrator Web Server selecciona automáticamente el puerto predeterminado (5986) o puede especificar un puerto alternativo.
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 mediante 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 cómo configurar usuarios nuevos.

1. Abra el explorador web.
2. En el campo Dirección, escriba uno de los siguientes valores:
   - `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 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

Este inicio de sesión está disponible solo 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 de **Server Administrator** del escritorio. Aparecerá la página de inicio de sesión remoto.

   PRECAUCIÓN: La pantalla de inicio de sesión muestra la casilla Ignorar advertencias 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 conectarse mediante 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 versión 3.0 y 3.5 o Microsoft Internet Explorer versión 7.0 o 8.0, es posible que aparezca una página intermedia de advertencia que muestre un problema con el certificado de seguridad. Para garantizar la seguridad del sistema, se recomienda que genere un nuevo certificado X.509, que utilice nuevamente un certificado X.509 existente, o bien, que importe una cadena de certificados de una entidad de certificación (CA). Para evitar tales mensajes de advertencia sobre el certificado, el certificado utilizado debe ser de 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 en el sistema administrado es válida y aún así Server Administrator Web Server registra un error de certificado no confiable, aún puede hacer que la CA del sistema administrado sea confiable al utilizar 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 le permite otorgar acceso a Server Administrator; lo cual le permite agregar y controlar usuarios y privilegios de Server Administrator a usuarios existentes en el software de Active Directory. Para obtener más información, consulte "Using Microsoft Active Directory" (Uso de Microsoft Active

Directory) en la *Server Administrator Installation Guide (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, debe tener una cuenta en la máquina con los privilegios adecuados (usuario, usuario avanzado o administrador). Los demás usuarios se autentican mediante Active Directory de Microsoft. Para iniciar Server Administrator utilizando la autentificación de inicio de sesión único mediante Active Directory de Microsoft, también se deben aplicar los siguientes parámetros:

```
authType=ntlm&application=[nombre del complemento]
```

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 OpenManage Essentials) tengan acceso directo a las páginas web de Server Administrator sin pasar por la página 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 **Nivel personalizado**.

   Para Windows Server 2003:

   a. En **Varios**, seleccione **Permitir Meta Refresh**.
   b. En **Secuencia de comandos ActiveX**, seleccione **Activar**.
   c. En **Secuencia de comandos ActiveX**, seleccione **Permitir la secuencia de comandos de los controles del explorador de web Internet Explorer**.
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. Para hacerlo, verifique 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 use los botones de la barra de herramientas del explorador web (como **Atrás** y **Actualizar**) mientras usa Server Administrator. Utilice 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 del 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.

Además, 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 6. 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
Módulo del servidor	Sistema modular
Sistema principal	Sistema modular
System	Sistema no modular
Chasis del sistema principal	Sistema no modular

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

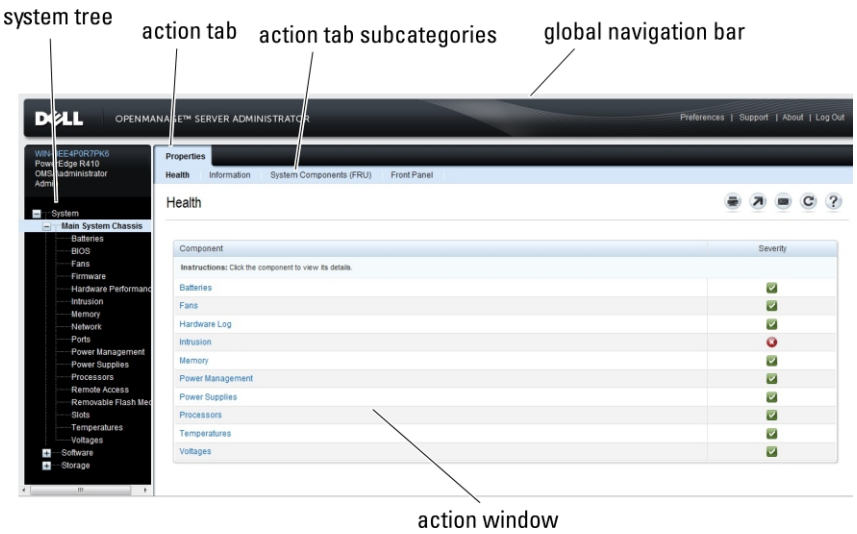

Ilustración 1. Ejemplo de la página de inicio de Server Administrator: sistema no modular

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

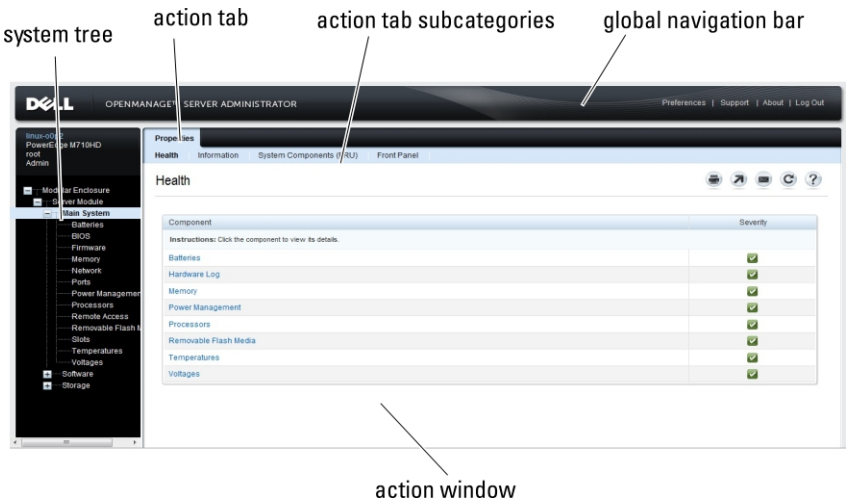

Ilustración 2. Ejemplo de la página de inicio de Server Administrator: sistema modular

Al hacer clic en un objeto del árbol del sistema, se abre la ventana de acciones correspondiente a ese objeto. Para navegar por la ventana de acciones, haga clic en las fichas de acción para seleccionar las categorías principales y haga clic en las subcategorías de la ficha de acción para acceder a información más detallada o a 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. Al hacer clic en un elemento subrayado, se crea una nueva área de datos en la ventana de acciones que contiene un nivel de detalles mayor. Por ejemplo, al hacer clic en **Chasis del sistema principal/Sistema principal** en la subcategoría **Condición** de la ficha de acción **Propiedades**, se enumera el estado de mantenimiento de todos los componentes supervisados que el objeto Chasis del sistema principal/Sistema principal contiene.

NOTA: Se requieren privilegios de administrador o usuario avanzado para ver la mayoría de los objetos del árbol del sistema, los componentes del sistema, las fichas de acción y las funciones del área de datos configurables. 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 en sistemas modulares y no modulares

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

Tabla 7. 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	✗	✓ (10° generación en adelante)
Intrusión	✗	✓
Memory (Memoria)	✓	✓
Network (Red)	✓	✓
Puertos	✓	✓
Administración de energía	✓	✓ (10° generación en adelante)
Procesadores	✓	✓
Acceso remoto	✓	✓
Medios flash extraíbles	✓	✓
Ranuras	✓	✓
Temperaturas	✓	✓
Voltajes	✓	✓

Características	Sistema modular	Sistema no modular
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 en el 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.
- Haga clic en **Acerca de** para mostrar la versión de Server Administrator y la información sobre derechos de autor.
- Haga clic en **Cerrar sesión** para finalizar la sesión actual del programa de Server Administrator.

Árbol del sistema

El árbol del sistema aparece a la izquierda de la página de inicio de Server Administrator y enumera los componentes del sistema que se pueden mostrar. Los componentes del sistema están clasificados por tipo de componente. Cuando expande el objeto principal conocido como **Gabinete modular → Módulo del servidor/sistema**, las principales categorías 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 bien, haga 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 se 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. El área de datos muestra la subcategoría preseleccionada de la primera ficha de acción del objeto seleccionado.

Por lo general, la subcategoría preseleccionada es la primera opción. Por ejemplo, cuando 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 **Condición** en el área de datos de la ventana.

Área de datos

El área de datos se ubica debajo de las fichas de acción a la derecha 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 se elije **BIOS** en el árbol del sistema, se 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/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 8. Indicadores de estado de los componentes del módulo del servidor/sistema

Descripción	Icono
El componente se encuentra en condición satisfactoria (normal).	
El componente presenta una condición de advertencia (no crítica). Una condición de advertencia 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 advertencia 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. La ventana **Registro**, por ejemplo, también contiene los botones de tareas **Guardar como** y **Borrar registro**.

- Al hacer clic en **Imprimir** () se imprime una copia de la ventana abierta en la impresora predeterminada.
- Al hacer 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 información acerca de cómo personalizar el delimitador separando los valores del campo de datos, consulte Configuración de las preferencias del usuario y del sistema.
- Al hacer 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 el destinatario de correo electrónico predeterminado, consulte Configuración de las preferencias del usuario y del sistema.
- Al hacer 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 sucesos del registro mostrados en el área de datos de la ventana de acciones.
- Al hacer clic en **Ayuda** ( ), se proporciona información detallada sobre una ventana específica o el botón de tareas que esté visualizando.

NOTA: Los botones **Exportar**, **Correo electrónico** y **Guardar como** solo son visibles 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

Al hacer 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 la CPU de un sistema.

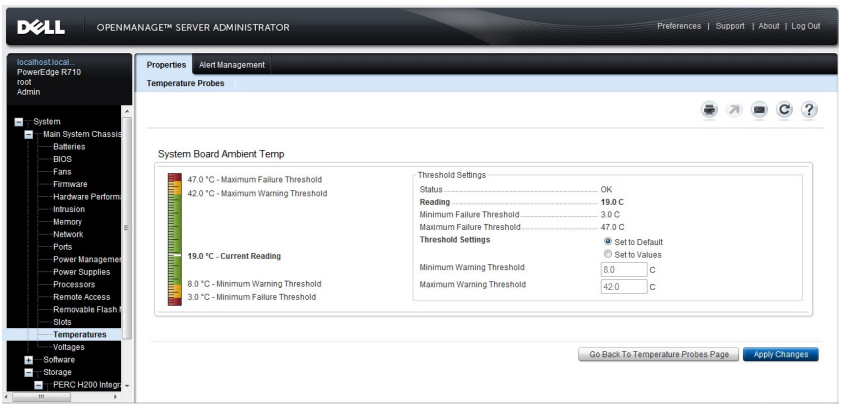

Ilustración 3. Indicador de medida

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 independiente de ayuda que contiene información detallada sobre la ventana específica visualizada. 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
- Server Administrator

Puede ver la ficha **Preferencias** después de iniciar sesión para administrar el 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 forma predeterminada la página de inicio de preferencias muestra la ventana Configuración de nodos en la ficha **Preferencias**.

Haga clic en el objeto Server Administrator para activar o desactivar el acceso de usuarios con privilegios de usuario o de usuario avanzado. Según los privilegios de 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.
- Configurar el tamaño del registro de comandos.
- Configurar SNMP.

Preferencias de Server Administrator Web Server

Al iniciar 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 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 Dell Systems Management

Configuración de las preferencias del usuario y del sistema

Las preferencias del sistema de puerto seguro y del usuario se pueden establecer desde 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 de la ventana adjunto 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 ingresar la dirección URL.

Sistema de puerto seguro

Siga estos pasos para configurar las preferencias del sistema de puerto seguro:

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. Seleccione **Activar** para permitir que se agote el tiempo de espera de Server Administrator si no hay interacción del usuario durante una cantidad especificada de minutos. Los usuarios en cuya sesión se le agota el tiempo de espera, deben iniciar sesión nuevamente para continuar. Seleccione **Desactivar** para desactivar la función **Tiempo de espera de la sesión (minutos)** de Server Administrator.
   - El campo **Puerto HTTPS** especifica el puerto seguro para Server Administrator. El puerto seguro predeterminado para Server Administrator es 1311.

     NOTA: Si se cambia el número de puerto por un número de puerto no válido o en uso, es posible que otras aplicaciones o exploradores no puedan acceder a Server Administrator en el sistema administrado. Para ver una lista de los puertos predeterminados, consulte la *Server Administrator Installation Guide (Guía de instalación de Server Administrator)*.
   - El campo **Dirección IP a la cual enlazar** especifica las direcciones IP para el sistema administrado a las cuales 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 a 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 forma predeterminada. Puede configurar varias direcciones de correo electrónico y utilizar una coma para separar cada una.
   - Los campos **Nombre del servidor SMTP (o dirección IP)** y **Sufijo DNS para el servidor SMTP** especifican el protocolo simple de transferencia de correo (SMTP) y el sufijo del servidor de nombre de dominio (DNS) de la empresa u organización. Para activar Server Administrator para el envío de correos electrónicos, debe escribir la dirección IP y el sufijo de DNS para el servidor SMTP de la empresa u organización en los campos adecuados.

     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 utilizado para separar los campos de datos en los archivos creados mediante el botón **Exportar**. El carácter **;** es el delimitador predeterminado. Otras opciones son **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|** y **,**.
   - El campo **Cifrado SSL** especifica los niveles de cifrado para las sesiones HTTPS protegidas. Los niveles de cifrado disponibles incluyen **Negociar automáticamente** y **128 bits o superior**.

     – **Negociar automáticamente**: permite la conexión procedente del explorador con cualquier nivel de cifrado. El explorador negocia automáticamente con Server Administrator Web Server y utiliza el nivel de cifrado más elevado disponible para la sesión. Los exploradores heredados con un cifrado de menor nivel también pueden conectarse a Server Administrator.

     – **128 bits o superior**: permite conexiones procedentes de exploradores con niveles de cifrado de 128 bits o superior. Uno de los siguientes conjuntos de cifrado es aplicable según el explorador para cualquiera de las sesiones establecidas:

     ```
     SSL_RSA_WITH_RC4_128_SHA
     ```

SSL_RSA_WITH_RC4_128_MD5

SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_DSS_WITH_AES_128_CBC_SHA

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

NOTA: La opción **128 bits o superior** no permite las conexiones procedentes de exploradores con niveles inferiores de cifrado SSL (por ejemplo, 40 bits y 56 bits).

- **Algoritmo de firma clave (para certificado autofirmado)**: permite seleccionar un algoritmo de firma admitido. Si selecciona **SHA 512** o **SHA 256**, asegúrese de que el explorador o sistema operativo admitan este algoritmo. Si selecciona una de estas opciones sin contar con un explorador o sistema operativo compatible, Server Administrator muestra el error `cannot display the webpage`. Este campo solamente se utiliza para certificados autofirmados y generados automáticamente. La lista desplegable aparece en gris si se importan o generan 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 de la lista desplegable.

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

NOTA: Si el nivel de cifrado está establecido en **128 bits o superior**, podrá acceder a la configuración de Server Administrator o modificarla a través de un explorador que tenga los mismos niveles de cifrado o un nivel mayor.

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 garantizar la identidad de un sistema remoto y para asegurar que la información intercambiada con dicho sistema no pueda ser vista ni cambiada por otros usuarios. 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 OMSA 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 sobre el host que la AC necesita para automatizar la creación de un certificado web SSL de confianza. Usted puede recuperar el archivo de CSR necesario a partir de las instrucciones que aparecen en la página Solicitud de firma de certificado (CSR) o si copia todo el texto del cuadro de texto de la página de CSR y lo pega en el formulario de envío de la AC. El texto debe estar en 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.

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

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 *Server Administrator Command Line Interface Guide* (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.

Además, los administradores del sistema 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 suceso de advertencia para ese componente (los valores de error mínimos y máximos los especifica el fabricante del sistema).
- Especificar cómo responde el sistema cuando ocurre un suceso de advertencia o error. Los usuarios pueden configurar las acciones que lleva a cabo un sistema en respuesta a las notificaciones de sucesos de advertencia 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 suceso.
- 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, si el sistema es arrendado o propio, etc.

NOTA: Debe configurar el servicio del protocolo simple de administración de red (SNMP) para aceptar los paquetes de SNMP para los sistemas administrados y los sistemas de administración de red que ejecutan Microsoft Windows Server 2003. Para obtener más información acerca de cómo configurar SNMP, consulte Configuración del agente SNMP en sistemas que ejecutan sistemas operativos Windows compatibles.

Administración del sistema

La página de inicio de Server Administrator muestra el objeto Sistema de la vista del árbol del sistema. De forma predeterminada, se abren los componentes **Condición** 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 visualizada. 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 la mayoría de los objetos del árbol del sistema, los componentes del sistema, las fichas de acción y las funciones del área de datos configurables. 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/sistema

El árbol del módulo del servidor/sistema de Server Administrator 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 están clasificados por tipo de componente. Cuando expande el objeto principal — **Gabinete modular** — **Módulo del servidor/sistema** — las categorías principales de componentes del sistema que se pueden mostrar 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 VMware ESX y ESXi versión 4.X y 5.X, algunas funciones que se encuentran disponibles en versiones anteriores de Server Administrator no se encuentran disponibles en esta versión. Estas incluyen:

- Información acerca de la compatibilidad de Fibre Channel sobre Ethernet (FCoE) y de la compatibilidad iSCSI sobre Ethernet (iSoE)
- 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 requieren privilegios de administrador o de 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 son configurables. De manera adicional, solamente los usuarios que se conectan con privilegios de administrador pueden acceder a las funciones esenciales del sistema, como la funcionalidad de apagado que se incluye 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 varios 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 es un sistema tan completo como 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 de 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/sistema

El objeto **Módulo del servidor/sistema** contiene tres grupos de componentes de sistema principales: Chasis del sistema principal/Sistema principal, Software y Almacenamiento. De forma predeterminada, la página de inicio de Server Administrator muestra el objeto **Sistema** de la vista de árbol del sistema. La mayoría de las funciones administrativas se pueden administrar en la ventana de acciones del objeto **Módulo del servidor/sistema**. La ventana de acciones del objeto **Módulo del servidor/sistema** tiene las siguientes fichas, según los privilegios de grupo del usuario: **Licencias**, **Propiedades**, **Apagado**, **Registros**, **Administración de alertas** y **Administración de sesiones**

Licensing

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 estado de la licencia, descripción de la licencia, id. de propiedad y fecha de expiración de la licencia.

  NOTA: Server Administrator admite la función de licencias en los sistemas PowerEdge de 12° generación y versiones posteriores. La función está disponible solo si está instalada la versión mínima requerida de iDRAC, iDRAC 1.30.30.

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 del sistema automática no estén disponibles cuando el temporizador de vigilancia del sistema operativo esté activado en el BIOS. Para configurar las opciones de recuperación automática, el temporizador de vigilancia del sistema operativo debe estar desactivado.

  NOTA: Es posible que las acciones de recuperación del sistema automática no se ejecuten exactamente por período de espera (n segundos) cuando el temporizador de vigilancia identifica un sistema que ha dejado de responder. El tiempo de ejecución de acción varía de n-h+1 a n+1 segundos donde n es el período de espera y h es el intervalo de latidos. El valor del intervalo de latidos es 7 segundos cuando n $\leq$ 30 y 15 segundos cuando n > 30.

  NOTA: La funcionalidad del temporizador de vigilancia no se puede garantizar cuando se produce un suceso de memoria incorregible en el sistema DRAM Bank_1. Si se produce un suceso de memoria incorregible en esta ubicación, es posible que el código de BIOS residente en este espacio esté dañado. Dado que la función del temporizador de vigilancia convoca al BIOS para efectuar el comportamiento de apagado o reinicio, es posible que la función no se ejecute correctamente. Si esto ocurre, debe reiniciar manualmente el sistema. El temporizador de vigilancia se puede configurar en 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 cuando un sensor de temperatura envíe un valor de advertencia 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

Subfichas: Hardware | Alerta | Comando

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

- Ver el registro de Embedded System Management (ESM) o el registro de sucesos del sistema (SEL) para obtener una lista de todos los sucesos relacionados con los componentes de hardware del sistema. El icono de indicador de estado que se encuentra junto al nombre del registro pasa del estado normal () al estado no crítico () cuando el archivo de registro alcanza el 80 % de la capacidad. En los sistemas Dell PowerEdge de 9° y 11° generación, el icono de indicador de estado que se encuentra junto al nombre del registro pasa al estado crítico () cuando el archivo de registro alcanza el 100 % de la capacidad.

  NOTA: Se recomienda borrar el registro de hardware cuando alcance el 80% de la capacidad. Si el registro tiene permitido alcanzar el 100% de la capacidad, se descartan los sucesos más recientes del registro.
- Ver el registro de alertas para obtener una lista de todos los sucesos 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 suceso de alerta y su descripción correspondiente, nivel de gravedad y causa, consulte la *Server Administrator Messages Reference Guide (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 por correo electrónico registros, consulte Registros de Server Administrator.

Administración de alertas

Subfichas: Acciones de alerta | Sucesos 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 advertencia o de error.
- Ver la configuración actual del filtro de sucesos de plataforma y establecer las acciones del filtro de sucesos de plataforma que desea realizar en caso de que el sensor de algún componente del sistema devuelva un valor de advertencia 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 suceso 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 alertas 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 suceso que corresponda en el nivel de gravedad seleccionado.

NOTA: Las acciones de alerta de todos los sensores de componentes del sistema potenciales 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/Sistema principal

Al hacer clic en el objeto **Chasis del sistema principal**/**Sistema principal** se pueden administrar los componentes de software y de hardware esenciales del sistema.

Los componentes que están disponibles son:

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

• Ranuras

• Temperaturas

• Voltajes

NOTA: El rendimiento de hardware solo se admite en sistemas Dell PowerEdge de 10° generación y posteriores. La opción **Fuentes de alimentación** no está disponible en Dell PowerEdge 1900. La administración de energía se admite en sistemas Dell PowerEdge de 10° generación y posteriores limitados. Las funciones de supervisión de fuentes de alimentación y supervisión de energía están disponibles solo para sistemas que tienen instaladas dos o más fuentes de alimentación redundantes que se pueden intercambiar directamente. Estas funciones no están disponibles para las fuentes de alimentación no redundantes instaladas en forma permanente que carecen de conjuntos de circuitos de administración de energía.

Propiedades del chasis del sistema principal/sistema principal

El módulo del servidor/sistema puede contener un chasis del sistema principal o varios chasis. El chasis del sistema principal o sistema principal contiene los componentes esenciales de un sistema. La ventana de acción 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:

- Ver el estado o la condición de los componentes de hardware y sensores. Cada componente que aparece en la lista tiene un icono Indicadores de estado de los componentes del módulo del servidor/sistema junto a su nombre.  indica que el componente se encuentra en buen estado (normal).  indica que el componente presenta una condición de advertencia (no crítica) y necesita una pronta atención.  indica que el componente presenta una condición de error (crítica) y requiere atención inmediata.  indica que no se conoce el estado del componente. Los componentes supervisados disponibles incluyen:

- Baterías
- Ventiladores
- Registro de hardware
- Intrusión
- Network (Red)
- Administración de energía
- Fuentes de alimentación
- Procesadores
- Temperaturas
- Voltajes

NOTA: Las baterías solo se admiten en sistemas Dell PowerEdge de 9° y 10° generación. La opción **Fuentes de alimentación** no está disponible en Dell PowerEdge 1900. La administración de energía se admite en sistemas Dell PowerEdge de 10° generación limitados. Las funciones **Supervisión de fuentes de alimentación** y **Supervisión de la alimentación** están disponibles solo para sistemas que tienen instaladas dos o más fuentes de alimentación redundantes que se pueden intercambiar directamente. Estas funciones no están disponibles para las fuentes de alimentación no redundantes instaladas de forma permanente que carecen de conjuntos de circuitos 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 de 12° generación, la pantalla **Componentes del sistema (FRU)** no aparece.

- Ver información sobre los atributos del chasis del sistema principal como nombre de host, versión de iDRAC, versión de Lifecycle Controller, modelo de chasis, seguro del chasis, etiqueta de servicio del chasis, código de servicio rápido y etiqueta de propiedad del chasis. El atributo Código de servicio rápido (ESC) es una conversión numérica de solo 11 dígitos de la etiqueta de servicio del sistema Dell. Cuando se llama a asistencia técnica de Dell, 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**)].
- Activar o desactivar los botones del panel frontal del sistema administrado, como el botón Energía y el botón Interrupción sin enmascaramiento (NMI) (si están presentes en el sistema). Además, seleccionar el nivel de acceso de seguridad de LCD del sistema administrado. La información de LCD del sistema administrado se puede seleccionar desde el menú desplegable. Puede además activar Indicación de sesión de KVM remoto desde la subficha **Panel frontal**.

Baterías

Haga clic en el objeto **Baterías** para ver la información sobre las baterías instaladas en el sistema. Las baterías mantienen la hora y la fecha cuando se apaga el 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: Información

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

Administración de alertas

En la ficha **Administración de alertas**, puede configurar las alertas que desea que se activen en caso de una advertencia de la batería o un suceso crítico o de error.

BIOS

Haga clic en el objeto **BIOS** para administrar las funciones clave del BIOS del sistema. El BIOS del sistema contiene programas almacenados en el conjunto de chips de la memoria flash que controlan la comunicación entre el microprocesador y los dispositivos periféricos, como el teclado y el adaptador de video, y otras funciones diferentes, como los mensajes del sistema. La ventana de acciones del objeto **BIOS** puede incluir las siguientes fichas, según los privilegios de 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 varias 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 , hyperThreading 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 libre de fallas de la redirección de consola. Además, puede configurar el dispositivo USB interno, la configuración de la controladora de la unidad óptica, el temporizador de vigilancia de la recuperación de sistema automática (ASR), el hipervisor incorporado y los puertos de red adicionales en la información de la placa base. También puede ver la configuración del módulo de plataforma segura (TPM) y del módulo criptográfico seguro (TCM).

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

Para sistemas de 12° generación, las funciones configurables del BIOS se agrupan como categorías específicas. Las categorías incluyen información del sistema, configuración de la memoria, configuración del perfil del sistema, configuración de inicio de la interfaz extensible del firmware unificada (UEFI), tarjetas del controlador de la interfaz de red, inicio único e inhabilitación de ranuras. Por ejemplo, en la página **Configuración del BIOS del sistema**, al hacer clic en el vínculo **Configuración de la memoria**, aparecen las funciones que pertenecen a la memoria del sistema. Puede ver o modificar la configuración si se desplaza a las categorías correspondientes.

Puede establecer una contraseña de configuración del BIOS en la página **Configuración del BIOS - Seguridad del sistema**. Debe introducir la contraseña para activar y modificar la configuración del BIOS. De lo contrario, la configuración del BIOS aparece en el modo de solo lectura. Debe reiniciar el sistema una vez establecida 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 NIC en 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 activar o desactivar las NIC. Se recomienda realizar la configuración de las NIC incorporadas mediante la pantalla Configuración del sistema que aparece al presionar <F2> mientras el sistema se está iniciando.

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 las medición de las rpm. Las sondas del ventilador le informan las rpm a Server Administrator Instrumentation Service.

Al seleccionar Ventiladores en el árbol de dispositivos, los detalles se muestran en el área de datos del panel derecho de la página de inicio de Server Administrator. La ventana de acción 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 tiene el sistema, como BMC o ESM. Algunos valores para los umbrales no se pueden editar en los 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.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para los ventiladores. Las capturas seleccionadas se desencadenan si el sistema genera un suceso correspondiente en el nivel de gravedad seleccionado.

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**.

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

Tabla 9. Valores posibles para el estado y causa de una sonda

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

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

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

Intrusión

Haga clic en el objeto **Intromisión** para administrar el estado de intromisión al chasis del sistema. Server Administrator supervisa el estado de intromisión como una medida de seguridad para impedir el acceso no autorizado a los componentes críticos del sistema. La intromisión al chasis indica que se está abriendo o se ha abierto la cubierta del chasis del sistema. La ventana de acciones del objeto **Intromisión** 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 intromisión al 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 advertencia o de error.
- Ver los umbrales actuales de alertas de capturas SNMP y establecer los niveles de umbrales de alertas para el sensor de intromisión. Las capturas seleccionadas se desencadenan si el sistema genera un suceso correspondiente 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 contando el 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 presentar 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 arreglos de memoria, la capacidad total de los arreglos de memoria, los detalles de 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 fila de dispositivos de memoria dinámica de acceso aleatorio (DRAM) que constan de 64 bits de datos por módulo de memoria DIMM. Los posibles valores de rango son `único`, `doble`, `quad`, `octal` y `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 encontrar el módulo de memoria con error.

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 módulo de memoria 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 los módulos de memoria. Las capturas seleccionadas se desencadenan si el sistema genera un suceso correspondiente 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: El orden según el cual se detectan los dispositivos no está garantizado para que coincida con el orden de puertos físicos del dispositivo. Haga clic en el hipervínculo en Nombre de la interfaz para ver la información de NIC.

En el caso de sistemas operativos ESX y 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 VMKernel (vmknic) en ESX y los dispositivos vmknic en ESXi.

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.

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: Los puertos USB de CMC conectados a servidores blade no están enumerados por OMSA.

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 alimentación están disponibles solo para sistemas que tienen instalados dos o más fuentes de alimentación redundantes que se pueden intercambiar directamente. Estas funciones no están disponibles para las fuentes de alimentación no redundantes instaladas de forma permanente que carecen de conjuntos de circuitos de administración de energía.

Supervisión

Subfichas: Consumo | Estadísticas

La ficha **Consumo** permite ver y administrar la información sobre consumo de alimentación 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** 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 sucesos como Advertencia 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 la alimentación solo estén disponibles en los sistemas activados con el bus de administración de la alimentación (PMBus).

Suministros de energía

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 suministros de energía y Supervisión de alimentación están disponibles solo para sistemas que tienen instalados dos o más suministros de energía redundantes que se pueden intercambiar directamente. Estas funciones no están disponibles para los suministros de energía no redundantes instaladas de forma permanente que carecen de conjuntos de circuitos 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.
- Comprobar el estado de los elementos de suministro de energía individuales, incluida la versión de firmware del suministro de energía, los vatios nominales de entrada y los vatios nominales de salida. El atributo de vatios nominales de entrada se muestra solo en los sistemas PMBus a partir de la 11° 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 suceso correspondiente 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. Un procesador es el chip informático principal dentro de un sistema que controla la interpretación y la ejecución de 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 advertencia 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).

Al seleccionar la ficha Acceso remoto, el usuario puede administrar las funciones de BMC/iDRAC, como la información general de BMC/iDRAC. Es posible además 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, BMC/iDRAC en una conexión de comunicación en serie en la LAN y los usuarios de BMC/iDRAC.

NOTA: BMC se admite en los sistemas Dell PowerEdge de 9° generación, mientras que iDRAC solo se admite en los sistemas Dell PowerEdge de 10° y 11° generación.

NOTA: Si una aplicación que no sea Server Administrator se usa para configurar BMC/iDRAC mientras 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 del sistema remota. 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 un 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.

NOTA: Los campos Activar NIC, Selección de NIC y Clave de cifrado solo se muestran en los sistemas Dell PowerEdge de 9° generación.

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.

NOTA: En los sistemas Dell PowerEdge de 9° generación:

- Se muestran diez identificaciones de usuario. Si una tarjeta de DRAC está instalada, se muestran 16 identificaciones de usuario.

- Se muestra la columna Carga de comunicación en serie en la LAN.

Medios flash extraíbles

Haga clic en el objeto **Medios flash extraíbles** para ver la condición y el estado de redundancia de los medios vFlash y los módulos SD internos. La ventana de acciones Medios flash extraíbles contiene 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 la configuración actual de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que la sonda de medios flash extraíbles devuelva un valor de advertencia 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 suceso 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 zócalos 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 de su 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 tiene el sistema, como BMC o ESM. Algunos valores para los umbrales no se pueden editar en sistemas basados en BMC. Cuando se asignan los valores para los umbrales de sondas, en algunos casos, Server Administrator redondea los valores mínimos o máximos que se introducen al valor más cercano que se puede asignar.

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 suceso correspondiente 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 decimal, solo se guardará el número entero anterior al lugar del decimal como el valor de 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 advertencia 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 advertencia 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 suceso correspondiente 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 incluye 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 del 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 incluye 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 la opción **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, en función de los privilegios de grupo del usuario: Propiedades.

Propiedades

Subficha: Condición

En la ficha **Propiedades**, puede ver la condición o el estado 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 el árbol del sistema aparece 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 están basadas 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
- Server Administrator

Configuración general

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

Subficha: Propiedades

User (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**.

- **Web Server**
- **Subfichas: Propiedades | Certificado X.509**

En la ficha Web Server, puede:

- Establecer las preferencias del servicio de conexión de DSM SA. Para obtener instrucciones sobre cómo configurar las preferencias del servidor, consulte Servicio de conexión y configuración de seguridad de la administración de servidores de Dell Systems Management.
- Configurar la dirección del servidor SMTP y la dirección IP de enlace ya sea en el modo de dirección IPv4 o IPv6.
- Realizar la administración de certificados X.509 mediante la generación de un nuevo certificado X. 509, la reutilización de un certificado X.509 existente o la importación de una cadena de certificados a partir de una entidad de certificación (CA). Para obtener más información acerca de la administración de certificados, consulte Administración de certificados X.509.

Server Administrator

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 presentar 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

Uso de Remote Access Controller

La controladora de administración de la placa base (BMC) de los sistemas Dell/Integrated Dell Remote Access Controller (iDRAC) supervisa el sistema para sucesos críticos mediante la comunicación con varios sensores en la placa del sistema y envía alertas y sucesos de registro cuando determinados parámetros superan sus umbrales predefinidos. BMC/iDRAC admite la especificación de la interfaz de administración de plataforma inteligente (IPMI) de la industria estándar, lo que permite configurar, supervisar y recuperar los sistemas de forma remota.

NOTA: Los sistemas Dell PowerEdge de 9° generación admiten la controladora de administración de la placa base (BMC), mientras que los sistemas Dell PowerEdge de 10° y 11° generación admiten Integrated Dell Remote Access Controller (iDRAC).

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 los sistemas Dell.

Al comunicarse con la controladora de administración de la placa base (BMC)/Integrated Dell Remote Access Controller (iDRAC) del sistema, es posible configurar DRAC para enviar alertas de correo electrónico para advertencias o errores relacionados con voltajes, temperaturas y velocidades de ventiladores. DRAC también registra los datos de sucesos y la pantalla de bloqueo más reciente (disponible únicamente en sistemas que ejecutan el sistema operativo Microsoft Windows) para ayudarlo a diagnosticar la posible causa del bloqueo del sistema.

Remote Access Controller proporciona acceso remoto a un sistema que no funciona, permitiéndole poner el sistema en funcionamiento lo más rápido posible. Remote Access Controller también proporciona 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 los bloqueos 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 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 BMC, consulte la *Dell OpenManage Baseboard Management Controller Utilities User's Guide (Guía del usuario de la controladora de administración de placa base Dell OpenManage)* en **dell.com/systemsecuritymanuals**.

NOTA: Para obtener más información sobre el uso de DRAC 5, consulte la *Dell Remote Access Controller 5 User's Guide (Guía de usuario de Dell Remote Access Controller 5)* en **dell.com/systemsecuritymanuals**.

NOTA: Para obtener información detallada sobre la configuración y el uso de iDRAC, consulte la *Integrated Dell Remote Access Controller User's Guide (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 10. 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 *Dell Systems Software Support Matrix (Matriz de compatibilidad de software de los sistemas Dell)* disponible en **dell.com/openmanagemanuals**.

Server Administrator permite acceso remoto dentro de banda a registros de sucesos, control de alimentación e información de estado de sensores y proporciona la capacidad para configurar BMC/iDRAC. Para administrar BMC/iDRAC y 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 sucesos 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 de BMC/iDRAC y DRAC también se pueden administrar mediante el comando de la interfaz de línea de comando (CLI) `omreport/omconfig chassis remoteaccess`.

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

NOTA: Los datos de BMC solamente se pueden ver en sistemas Dell PowerEdge de 9° generación.

Visualización de la información básica

Es posible ver información básica sobre BMC/iDRAC, la dirección IPv4 y DRAC. Asimismo, se puede restablecer la configuración de la controladora de acceso remoto a los valores predeterminados. Para hacerlo, tenga en cuenta lo siguiente:

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 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: Solamente 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** de 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 **Gabinete modular → Módulo del servidor/sistema → Chasis del sistema principal/ Sistema principal → Acceso remoto**.
2. Haga clic en la pestaña **Configuration (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 (esta opción está disponible en sistemas Dell PowerEdge de 9° generación cuando DRAC está instalado. Seleccione esta opción para asociar NIC. En sistemas Dell PowerEdge de 9° generación, puede asociar NIC para redundancia adicional).

   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 su puerta de enlace predeterminada es 192.168.20.1.

   NOTA: Si se configura DRAC para 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 al cambiar la dirección IP de la otra NIC.

   NOTA: Al cambiar la dirección IP de DRAC, se debe restablecer DRAC. 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° generación y versiones anteriores.

   - Opciones de red primaria y de conmutación por error

   Para los sistemas de 12° generación, las opciones de red primaria para **NIC** de administración remota (iDRAC7) son: **LOM1**, **LOM2**, **LOM3**, **LOM4** y **Dedicated** (Dedicado). Las opciones de red de conmutación por error son: **LOM1**, **LOM2**, **LOM3**, **LOM4**, **All LOMs** (Todos los LOM) y **None** (Ninguno).

   La opción dedicada está disponible cuando la licencia de Enterprise en iDRAC7 está presente y es válida.

   NOTA: El número de LOM varía según la configuración del sistema o del hardware.

   - Activar la IPMI en la LAN
   - Fuente de dirección IP
   - IP address (Dirección IP)
   - Máscara de subred
   - Dirección de puerta de enlace
   - Límite del nivel de privilegios del canal
   - Nueva clave de cifrado (esta opción está disponible en sistemas Dell PowerEdge de 9° generación).
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.

   - Activar identificación de VLAN
   - Id. de VLAN
   - Priority (Prioridad)

6. Configure las siguientes propiedades de IPv4:
   - Fuente de dirección IP
   - IP address (Dirección IP)
   - Máscara de subred
   - Dirección de puerta de enlace
7. Configure las siguientes propiedades de IPv6:
   - Fuente de dirección IP
   - IP address (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 la transmisión de mensajes de administración de interfaz de plataforma inteligente (IPMI) a través del puerto serie con caracteres ASCII imprimibles. El modo de terminal también admite una cantidad limitada de comandos de texto para admitir entornos heredados basados en texto. Este entorno está diseñado para permitir el uso de un simple terminal 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
   - Nueva secuencia de línea de entrada
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 ficha **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 ficha **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 **Configuration (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 *Dell License Manager User's Guide (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.
   - En sistemas Dell PowerEdge de 9° generación, seleccione **Activar comunicación en serie en la LAN** para activar esta comunicación.
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 sucesos de plataforma

Para configurar las funciones BMC más relevantes, 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 sobre sucesos de plataforma específicos. Puede seleccionar esos sucesos para los que desea realizar acciones de apagado y generar alertas para acciones específicas. Además, puede enviar alertas para destinos de direcciones IP específicos de su elección.

   NOTA: Para configurar las alertas de PEF de la BMC, se debe iniciar sesión con privilegios de administrador.

   NOTA: La configuración **Activar las alertas de filtro de sucesos de plataforma** permite desactivar o activar la generación de alertas de PEF. Es independiente de la configuración individual de alertas de sucesos de plataforma.

   NOTA: Las funciones **Advertencia de sonda de alimentación del sistema** y **Error en sonda de alimentación del sistema** no se admiten en los sistemas Dell PowerEdge que no son compatibles con PMBus, a pesar de que Server Administrator permita configurarlas.

   NOTA: En los sistemas Dell PowerEdge 1900, no se admiten los filtros de sucesos de plataforma Advertencia PS/VRM/D2D, Error PS/VRM/D2D y Suministro de energía ausente, aún cuando Server Administrator permita configurar estos filtros de sucesos.

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

   La ventana **Establecer sucesos de plataforma** le permite especificar las acciones que se deberán realizar si el sistema se debe apagar 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: Si selecciona una acción de apagado de suceso de plataforma que no sea la opción Ninguno ni la opción Reducción de la alimentación, el sistema se apagará de forma forzada cuando se produzca el suceso especificado. El firmware iniciará este apagado y se realizará sin apagar primero el sistema operativo ni las aplicaciones en ejecución.

     NOTA: No todos los sistemas admiten la reducción de la alimentación. Las funciones Supervisión del suministro de energía y Supervisión de alimentación están disponibles únicamente para sistemas que tengan instalados dos o más suministros de energía redundantes con intercambio directo. Estas funciones no están disponibles para suministros de energía no redundantes instalados de forma permanente que carecen de conjuntos de circuitos para la administración de la alimentación.
6. Seleccione la casilla **Generar alerta** para enviar las alertas que desea.

   NOTA: Para generar una alerta, debe seleccionar tanto el valor **Generar alerta** como el valor **Activar 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 sucesos de plataforma

Puede también usar la ventana Filtros del suceso de plataforma para seleccionar un destino donde se envíe una alerta de suceso de plataforma. Según la cantidad de destinos que se muestren, es posible 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 introducir una dirección IP individual para el destino. Esta dirección IP es la dirección a la que se envía la alerta del suceso de plataforma.

   NOTA: En los sistemas de 12° 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 **Apply (Aplicar)**.
7. Haga clic en **Volver a la página de sucesos de plataforma** para volver a la ventana **Filtros del suceso de plataforma**.

6

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 *Server Administrator Command Line Interface Guide (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 más información sobre la ventana específica que está 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.

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 soporte el 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 especificar.
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 sucesos del registro.
Guardar como	Para guardar el contenido del registro en un archivo **.zip**.

Nombre	Descripción
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 sistemas Dell PowerEdge de 9° y 11° generación, use el registro de hardware para buscar problemas potenciales con los componentes de hardware del sistema. El indicador de estado del registro de hardware pasa al estado crítico ( ) cuando el archivo de registro alcanza el 100% de la capacidad. Hay dos registros de hardware disponibles, según el sistema: el registro de Embedded System Management (ESM) y el registro de sucesos del sistema (SEL). El registro de ESM y SEL constituyen cada uno un conjunto de instrucciones incorporadas que pueden enviar mensajes de estado de hardware al software de administración de sistemas. Cada componente enumerado en los registros tiene un icono de indicador de estado junto a su nombre. La siguiente tabla enumera los indicadores de estado.

Tabla 12. Indicadores de estado del registro de hardware

Status (Estado)	Descripción
Una marca de color 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 advertencia (no crítica) y necesita una pronta atención.
Una X de color rojo ( )	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 suceso
- La fecha y hora en la que se capturó el suceso
- Una descripción del suceso

Mantenimiento del registro de hardware

El icono de indicador de estado ubicado 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 el 80% de la capacidad. Asegúrese de borrar el registro de hardware cuando alcance el 80% de la capacidad. Si se permite que el registro alcance el 100% de la capacidad, se descartan los sucesos más recientes 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.

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

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

La información que aparece en el registro de alertas incluye:

- El nivel de gravedad del suceso
- La id. del suceso
- La fecha y hora en la que se capturó el suceso
- La categoría del suceso
- Una descripción del suceso

NOTA: Es posible que el historial del registro se requiera para solucionar futuros problemas y realizar diagnósticos. Por lo tanto, se recomienda guardar los archivos de registro.

NOTA: OMSA 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 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 *Server Administrator Messages Reference Guide (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 los usuarios de Server Administrator emiten. 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 la hora en 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 solucionar futuros problemas y realizar diagnósticos. Por lo tanto, se recomienda guardar los archivos de registro.

7

Establecimiento de acciones de alerta

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

Al establecer acciones de alerta para un suceso, es posible 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 cuando se ejecuta el sistema X Window, se debe iniciar **xconsole** o **xterm -C** antes de que ocurra el suceso. Para ver el mensaje de alerta en sistemas SUSE Linux Enterprise Server cuando se ejecuta el sistema X Window, se debe iniciar un terminal como **xterm -C** antes de que ocurra el suceso.

Cuando establece acciones de alerta para un suceso, puede especificar la acción para **difundir un mensaje**. Para realizar esta acción, Server Administrator ejecuta el comando wall, que envía el mensaje a todos los usuarios conectados con su permiso para mensajes configurado en **Sí**. Si el sistema de Server Administrator está ejecutando un sistema X Windows, el mensaje no se mostrará de forma predeterminada. Para ver el mensaje de difusión mientras se ejecuta el sistema X Windows, debe iniciar un terminal, como **xterm** o **gnome-terminal**, antes de que se produzca el suceso.

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

- No especifique aplicaciones basadas en el sistema X Windows, ya que Server Administrator no puede ejecutar esas aplicaciones adecuadamente.
- No especifique aplicaciones que requieran que el usuario introduzca información, ya que Server Administrator no puede ejecutar esas aplicaciones correctamente.
- Redirija **stdout** y **stderr** a un archivo cuando especifique la aplicación, de manera que pueda ver todos los mensajes de salida o de error.
- Si desea ejecutar varias aplicaciones (o comandos) para una alerta, cree una secuencia de comandos e inserte 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 la aplicación ps, redirige stdout al archivo **/tmp/psout.txt** y redirige **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 de SUSE Linux Enterprise Server, y el administrador, con el asunto **Server Alert** (Alerta de servidor). El usuario debe crear el archivo **/tmp/**

alertmsg.txt antes de que se produzca el suceso. Además, **stdout** y **stderr** se redirigen al archivo **/tmp/mailout.txt** en caso de que se produzca un error.

Establecimiento de acciones de alerta en Microsoft Windows Server 2003 y Windows Server 2008

Cuando se especifican las acciones de alerta, la función Ejecutar aplicación no interpreta automáticamente las secuencias de comandos de Visual Basic, aunque se puede ejecutar un archivo `.cmd`, `.com`, .bat o .exe mediante la especificación del archivo como acción de alerta.

Para resolver este problema, en primer lugar invoque al procesador de comandos `cmd.exe` para iniciar su secuencia de comandos. Por ejemplo, el valor de la acción de alerta para ejecutar una aplicación puede configurarse de la siguiente manera:

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

donde `d:\example\example1.vbs` es la ruta completa del archivo de secuencia de comandos.

No establezca una ruta a una aplicación interactiva (una aplicación que tenga una interfaz gráfica de usuario o que requiera que el usuario introduzca información) en el campo Ruta de acceso absoluta a la aplicación. Es posible que la aplicación interactiva no funcione correctamente en algunos sistemas operativos.

NOTA: Debe especificar la ruta completa para los archivos **cmd.exe** y de secuencia de comandos.

NOTA: No se admite Microsoft Windows 2003 en los sistemas de 12° generación.

Definición de ejecución de aplicaciones para acciones de alerta en Windows Server 2008

Por razones de seguridad, Windows Server 2008 está configurado para no admitir servicios interactivos. Cuando un servicio se instala como servicio interactivo en Windows Server 2008, el sistema operativo registra un mensaje de error en el registro del sistema Windows acerca del servicio identificado como servicio interactivo.

Cuando usa Server Administrator para configurar acciones de alerta para un suceso, puede especificar la acción para ejecutar una aplicación. Para que las aplicaciones interactivas ejecuten adecuadamente las acciones de alerta, el servicio de administrador de datos de Dell Systems Management Server Administrator (DSM SA) debe configurarse como un servicio interactivo. Entre las aplicaciones interactivas, pueden mencionarse a aquellas que tienen una interfaz gráfica de usuario (GUI) o que requieran que el usuario introduzca algún tipo de datos, como en el caso del comando pause en un fichero.

Cuando Server Administrator está instalado en Microsoft Windows Server 2008, el servicio de administrador de datos de DSM SA se instala como servicio no interactivo; es decir, se configura de modo tal que no pueda interactuar con el escritorio en forma predeterminada. Esto significa que las aplicaciones interactivas no se ejecutarán correctamente cuando se ejecuten para una acción de alerta. Si en esa situación se ejecuta una aplicación interactiva para una acción de alerta, la aplicación queda suspendida y a la espera del ingreso de datos. El indicador o la interfaz de la aplicación no son visibles y

se mantienen ocultos incluso después de que se inicie el servicio de detección de servicios interactivos. La ficha **Procesos** del administrador de tareas muestra una entrada de procesos de aplicación para cada ejecución de la aplicación interactiva.

Si tiene que ejecutar una aplicación interactiva para una acción de alerta en Microsoft Windows Server 2008, debe configurar el servicio de administrador de datos de DSM SA de modo que pueda interactuar con el escritorio y activar servicios interactivos.

Para habilitar la interacción con el escritorio:

- Haga clic con el botón derecho del mouse en el servicio de administrador de datos de DSM SA en el panel de control **Servicios** y seleccione **Propiedades**.
- En la ficha **Inicio de sesión**, active la opción **Permitir que el servicio interactúe con el escritorio** y haga clic en **Aceptar**.
- Reinicie el servicio Administrador de datos de DSM SA para que el cambio tenga efecto.
- Asegúrese de que el servicio de **detección de servicios interactivos** se esté ejecutando.

Cuando se reinicie el servicio de administrador de datos de DSM SA con este cambio, el administrador de control de servicio registrará el siguiente mensaje en el registro del sistema:

```
El servicio de administrador de datos de DSM SA está identificado como un
servicio interactivo. Al activar el servicio de detección de servicios
interactivos, se permite que el servicio de administrador de datos de DSM SA
ejecute aplicaciones interactivas correctamente para una acción de alerta.
```

Una vez efectuados estos cambios, el sistema operativo mostrará el cuadro de diálogo **Detección de diálogo de servicios interactivos** a fin de brindar acceso a la interfaz o al indicador de la aplicación interactiva.

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

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

Tabla 13. Sucesos de alerta de PEF

Suceso	Descripción
Falla de sonda del ventilador	El ventilador está funcionando muy lentamente o no está funcionando en absoluto.
Falla 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.
Falla 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.
Falla de sonda de temperatura	La temperatura es demasiado alta o demasiado baja para una operación adecuada.
Intromisión al chasis detectada	El chasis del sistema se ha abierto.

Suceso	Descripción
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.
Advertencia del procesador	Un procesador se está ejecutando con un rendimiento o a una velocidad menor al óptimo.
Falla 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 falla 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.
Advertencia de sonda de alimentación del sistema	El nivel de consumo de la alimentación se aproxima al umbral de error.
Falla de sonda de la alimentación del sistema	El nivel de consumo de alimentación 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.
Advertencia 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.
Advertencia 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 `SELinux is set to enforced mode`, el servicio de conexión de Dell Systems Management Server Administrator (SM SA) no se inicia. Realice uno de los siguientes pasos para iniciar este servicio:

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

  ```
  setsebool allow_execstack on
  ```

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

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 ESX/ESXi. Para obtener información sobre cómo activar los servicios de Server Administrator en el sistema VMware ESX/ESXi, consulte la *Server Administrator Installation Guide (Guía de instalación de Server Administrator)*, en **dell.com/openmanagemanuals**.
- El servicio Small Footprint CIM Broker Daemon (SFCBD) del sistema VMware ESX/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 *Server Administrator Installation Guide (Guía de instalación de Server Administrator)*, disponible en **dell.com/openmanagemanuals**.
- Se produce un error de autentificación al conectarse a un sistema operativo VMware ESXi 4.1/5.0, que puede producirse por cualquiera de los siguientes motivos:

  a. 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.

b. La contraseña se cambia mientras se está conectado a Server Administrator.

c. Inicia sesión en Server Administrator como un 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

Puede corregir una instalación defectuosa si fuerza una reinstalación y después desinstala 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 que se instalaron originalmente. Si no está seguro de las funciones que se instalaron, seleccione todas las funciones y realice 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 14. Servicios de Server Administrator

Nombre del servicio	Descripción	Impacto del error	Mecanismo de recuperación	Gravedad
Windows: servicio de conexión de SM SA Linux: `dsm_om_connsvc` (este servicio está instalado 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 operaciones 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	Ejecuta el recopilador de	Las actualizaciones de software no se	Reinicie el servicio	Aviso

Nombre del servicio	Descripción	Impacto del error	Mecanismo de recuperación	Gravedad
SA Linux: `dsm_om_shrsvc` (este servicio se ejecuta en el sistema administrado).	inventarios en el inicio para efectuar 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 (Dell System Management Console) y Dell IT Assistant (ITA).	pueden efectuar mediante ITA. Sin embargo, las actualizaciones aún se pueden realizar de forma local y fuera de Server Administrator mediante Dell Update Packages individuales. Las actualizaciones aún se pueden realizar mediante herramientas de terceros (por ejemplo, MSSMS, Altiris y Novell ZENworks).		

NOTA: OMSA 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 OMSA se reinician manualmente o cuando el sensor de dispositivo aún indica un estado no normal cuando los servicios de OMSA 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 OMSA (64 bits).

Windows: administrador de sucesos de SM SA Linux: `dsm_sa_eventmgrd` (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 sucesos de SM SA (Windows) Linux: `dsm_sa_eventmgrd` (alojado en el servicio dataeng)	Proporciona el servicio de registro de sucesos de archivos y sistema operativo para la administración de	Si se detiene este servicio, no funcionan correctamente las funciones de	Reinicie el servicio	Aviso

Nombre del servicio	Descripción	Impacto del error	Mecanismo de recuperación	Gravedad
(este servicio se ejecuta en el sistema administrado).	sistemas, y también es usado por analizadores de registros de sucesos.	registro de sucesos.		
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. **¿Por qué la funcionalidad de reinicio del host de ESXi 4.x (4.0 U3) y ESXi 5.x falla desde Server Administrator?**

   La causa de este problema es la clave de licencia independiente de VMware (SAL). Para obtener más información, consulte el artículo de la base de conocimientos en **kb.vmware.com/kb/kb1026060**.

2. **¿Cuáles son las tareas que se deben realizar después de agregar un sistema operativo VMware ESX 4.0 U3 o ESX 4.1 U2 al dominio de Active Directory?**

   Después de agregar un sistema operativo VMware ESX 4.0 U3 y ESX 4.1 U2 al dominio Active Directory, un usuario de Active Directory debe hacer lo siguiente:

   a. Iniciar sesión en Server Administrator en el sistema que ejecuta el sistema operativo VMware ESX 4.0 U3 y ESX 4.1 U2 y reiniciar el servicio de conexión de DSM SA.
   b. Iniciar sesión en el nodo remoto mientras usa el sistema operativo VMware ESX 4.0 U3 y ESX 4.1 U2 como un agente de Remote Enablement. Esperar aproximadamente 5 minutos para que el proceso sfcbd agregue el permiso al nuevo usuario.

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

   Para instalar Server Administrator, debe contar con privilegios de nivel de administrador. Los usuarios y los usuarios avanzados no tienen permisos para instalar Server Administrator.

4. **¿Existe una ruta de actualización requerida para instalar Server Administrator?**

   Para sistemas que ejecutan Server Administrator versión 4.3, debe actualizar a la versión 6.*x* y después a la versión 7.*x*. Para sistemas que ejecutan una versión anterior a 4.3, debe actualizar a la versión 4.3, después a la versión 6.*x* y después a la versión 7.*x* (*x* indica la versión de Server Administrator a la cual desea actualizar).

5. **¿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.

6. **¿Cómo puedo saber cuál es la versión de Server Administrator que se ejecuta en mi sistema?**

   Después de iniciar sesión en Server Administrator, navegue a **Propiedades** → **Resumen**. Puede encontrar la versión de Server Administrator instalada en el sistema en la columna **Systems Management**.

7. **¿Existen otros puertos que pueden ser utilizados por los usuarios además del puerto 1311?**

   Sí, puede establecer el puerto https preferido. Navegue hasta **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.

8. **¿Puedo instalar Server Administrator en Fedora, College Linux, Mint, Ubuntu, Sabayon o PClinux?**

   No. Server Administrator no admite ninguno de estos sistemas operativos.

9. **¿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.

10. **¿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 Windows Server), el sistema puede configurarse con SNMP y/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.

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

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

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

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

13. **¿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 "Using Microsoft Active Directory" (Uso de Microsoft Active Directory) en la *Server Administrator Installation Guide (Guía de instalación de Server Administrator)* disponible en **dell.com/openmanagemanuals**.

14. **¿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:

    Para 32 bits:

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

    Para 64 bits:

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

15. **¿Por qué el sistema operativo Red Hat Enterprise Linux 5.9 (de 32 bits) no puede detectar la tarjeta Emulex después de instalar los controladores Emulex?**

    En sistemas que ejecutan el sistema operativo Red Hat Enterprise Linux 5.9 (32 bits), el controlador Emulex depende de los siguientes RPM:

    - kernel-headers-2.6.18-346.el5.i386.rpm
    - glibc-headers-2.5-107.i386.rpm
    - glibc-devel-2.5-107.i386.rpm
    - gcc-4.1.2-54.el5.i386.rpm

    Si alguno de los RPM mencionados arriba no están, el sistema experimenta problemas al detectar los adaptadores de red Emulex.