Dell OpenManage Server Administrator Versión 6.3 Guía del usuario

Notas y precauciones

NOTA: Una NOTA proporciona información importante que le ayudará a utilizar mejor el ordenador.

PRECAUCIÓN: Un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, e informa de cómo evitar el problema.

Julio de 2010

Regresar a la página de contenido

Establecimiento de acciones de alerta

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

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

Cuando se establecen acciones de alerta para un suceso, se puede especificar la acción de **Mostrar una alerta en el servidor.** Para realizar esta acción, Server Administrator envía un mensaje a **/dev/console**. Si el sistema Server Administrator está ejecutando un sistema X Window, no verá el mensaje de manera predeterminada. Para ver el mensaje de alerta en un sistema Red Hat Enterprise Linux cuando el sistema X Window se está ejecutando, debe iniciar **xconsole** o **xterm -C** antes de que ocurra el suceso. Para ver el mensaje de alerta en un sistema SUSE Linux Enterprise Server cuando el sistema X Window se está ejecutando, debe iniciar **xterm -C** antes de que ocurra el suceso.

Al establecer las acciones de alerta para un suceso, se puede especificar la acción de **Difundir un mensaje**. Para realizar esta acción, Server Administrator ejecuta el comando **wall**, que envía el mensaje a todos los que están conectados con el permiso para mensajes establecido en **Sí**. Si el sistema Server Administrator está ejecutando un sistema X Window, no verá el mensaje de manera predeterminada. Para ver el mensaje de difusión cuando el sistema X Window se está ejecutando, debe iniciar un terminal, por ejemplo **xterm** o **gnome-terminal**, antes de que el suceso ocurra.

Al establecer las acciones de alerta para un suceso, se puede especificar la acción de **Ejecutar una aplicación**. Existen limitaciones en las aplicaciones que Server Administrator puede ejecutar. Siga estas pautas para garantizar 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 para hacer eso y escriba la ruta de acceso completa al archivo que contiene 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 contenido en el archivo **/tmp/alertmsg.txt** al usuario de Red Hat Enterprise Linux o al administrador y usuario de SUSE Linux Enterprise Server, con el asunto **Server Alert**. El archivo **/tmp/alertmsg.txt** debe ser creado por el usuario antes de que ocurra el suceso. Además, **stdout** y **stderr** se redirigen al archivo **/tmp/mailout.txt** en caso de que se presente un error.

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

Cuando se especifican acciones de alerta, la función Ejecutar aplicación no interpreta automáticamente las secuencias de comandos de Visual Basic, aunque es posible ejecutar un archivo `.cmd`, `.com`, `.bat` o `.exe` con sólo especificar el archivo como acción de alerta.

Para resolver este problema, ejecute primero el procesador de comando `cmd.exe` para iniciar la secuencia de comandos. Por ejemplo, el valor de la acción de alerta para ejecutar una aplicación se puede definir 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 de acceso para una aplicación interactiva (una aplicación que tiene una interfaz gráfica del usuario o que requiere de respuestas del usuario) en el campo Ruta de acceso absoluta a la aplicación. Es posible que la aplicación interactiva no funcione como se espera en algunos sistemas operativos.

NOTA: Se debe especificar la ruta de acceso completa del archivo cmd.exe y del archivo de secuencia de comandos.

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

Por motivos de seguridad, Windows Server 2008 está configurado para no permitir servicios interactivos. Cuando se instala un servicio como servicio interactivo en Windows Server 2008, el sistema operativo registra un mensaje de error en el registro del sistema de Windows que indica que el servicio se estableció como interactivo.

Al utilizar Server Administrator para configurar acciones de alerta para un suceso, se puede especificar la acción para *Ejecutar una aplicación*. Para que las aplicaciones interactivas se ejecuten correctamente para una acción de alerta, el servicio Administrador de datos de Dell Systems Management Server Administrator (DSM SA) debe estar configurado como servicio interactivo. Un ejemplo de aplicación interactiva son las aplicaciones con una interfaz gráfica de usuario (GUI) o las que solicitan que el usuario introduzca algún tipo de datos, como el comando *pause* de un archivo de proceso por lotes.

Cuando se instala Server Administrator en Microsoft Windows Server 2008, el servicio Administrador de datos de DSM SA se instala como servicio no interactivo; es decir, está configurado de modo tal que no pueda interactuar con el escritorio de manera predeterminada. Esto significa que las aplicaciones interactivas no se ejecutarán como corresponde cuando se utilicen para una acción de alerta. Si se ejecuta una aplicación interactiva para una acción de alerta en esta situación, la aplicación se suspende y queda a la espera de una entrada. La interfaz o el indicador de la aplicación no estarán visibles y se mantendrán en ese estado incluso después de iniciar 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 Administrador de datos de DSM SA de modo que pueda interactuar con el escritorio.

Para habilitar la interacción con el escritorio:

1. Haga clic con el botón derecho del mouse en el servicio Administrador de datos de DSM SA en el **panel** de **Control de servicios** y seleccione Propiedades.
2. En la ficha **Inicio de sesión**, active la opción **Permitir que el servicio interactúe con el escritorio** y haga clic en **Aceptar**.
3. Reinicie el servicio Administrador de datos de DSM SA para que el cambio tenga efecto.

Cuando se reinicia el servicio Administrador de datos de SA de DSM después de este cambio, el Administrador de control de servicios registra el siguiente mensaje en el registro del sistema: `The DSM SA Data Manager service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.(El servicio Administrador de datos de SA de DSM se marcó como servicio interactivo. Sin embargo, el sistema está configurado para no permitir los servicios interactivos.) Es posible que este servicio no funcione correctamente`). Este cambio permite que el servicio Administrador de datos de SA de DSM ejecute aplicaciones interactivas de manera adecuada para una acción de alerta. Asegúrese también de que la detección de servicios interactivos esté ejecutándose, a fin de poder ver la interfaz o el indicador en la aplicación interactiva. 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 el indicador de la aplicación interactiva.

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

Todos los mensajes de Filtro de sucesos de plataforma (PEF), junto con una descripción de cada suceso, aparecen en Tabla 7-1.

Tabla 7-1. 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.
Falla de sonda de voltaje discreto	El voltaje es demasiado bajo para una operación adecuada.
Advertencia 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.
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.
Advertencia PPS/VRM/CCaCC	El suministro de energía, el módulo regulador de voltaje o el convertidor de corriente continua a corriente continua tienen una condición de falla pendiente.
Falla del suministro de energía/VRM/D2D	El suministro de energía, el módulo regulador de voltaje o el convertidor de CC a CC han fallado.
El registro de hardware está lleno o se ha vaciado	Un registro de hardware lleno o vacío requiere la atención del administrador.
Recuperación automática del sistema	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 falla.
Falla de la sonda de alimentación del sistema	El nivel de consumo de alimentación ha superado el máximo límite admisible y ha producido una falla.
Advertencia de unidad extraíble presente	La unidad flash extraíble está presente.
Falla de unidad flash extraíble	La unidad flash extraíble tiene una condición de falla pendiente.
Advertencia de unidad flash extraíble	La unidad flash extraíble está presente.

Interpretación de nombres de servicio

El archivo ejecutable del servicio y los nombres de pantalla de los servicios siguientes han cambiado:

Tabla 7-2. Nombres de servicios

Propósito	Nombre del servicio	Versión anterior (anterior a 5.0)	Versión actual
Web Server	Nombre de pantalla	Puerto seguro Servidor	Servicio de conexión de DSM SA
	Nombre del archivo ejecutable	Omaws[32|64]	dsm_om_connsvc
			dsm_om_connsvc
Programación o notificación	Nombre de pantalla	Servicios Comunes OM	Servicios compartidos de DSM SA
	Nombre del archivo ejecutable	Omsad[32|64]	dsm_om_shrsvc
			dsm_om_shrsvc

Regresar a la página de contenido

Regresar a la página de contenido

Solución de problemas

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Falla del servicio de conexión

En Red Hat Enterprise Linux, cuando SELinux se establece en modo Forzado, el servicio de conexión de Dell Systems Management Server Administrator (DSM SA) falla al iniciarse. Realice alguno de los siguientes pasos e inicie el servicio:

- Establezca SELinux en modo Desactivado o en modo Permisivo.
- Cambie la propiedad **allow_execstack** de SELinux al estado **Encendido**. Ejecute el comando siguiente:

  ```
  setsebool allow_execstack on
  ```

- Cambie el contexto de seguridad del servicio de conexión de DSM SA. Ejecute el comando siguiente:

  ```
  chcon -t unconfined_execmem_t /opt/dell/srvadmin/sbin/dsm_om_connsvcd
  ```

Escenarios de errores de inicio de sesión

No podrá iniciar sesión en Managed System si:

- Introduce una dirección IP incorrecta/no válida.
- Introduce credenciales incorrectas (nombre de usuario y contraseña).
- Managed System está apagado.
- No es posible acceder a Managed System debido a una dirección IP no válida o un error de DNS.
- Managed System 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. Consulte la *Guía de instalación de Dell OpenManage Server Administrator* para obtener información sobre cómo activar los servicios de Server Administrator en el sistema VMware ESX/ESXi.
- El servicio Small Footprint CIM Broker Daemon (SFCBD) del sistema VMware ESX/ESXi no se está ejecutando.
- El servicio de administración de Web Server de Managed System no se está ejecutando.
- Se introdujo la dirección IP de Managed System sin el nombre del host y no se ha seleccionado la casilla **Ignorar advertencias de certificado**.
- La función de autorización WinRM (Remote Enablement) no está configurada en Managed System. Para obtener información sobre esta función, consulte la *Guía de instalación de Dell OpenManage Server Administrator*.
- Se produce una falla de autentificación al conectarse a un sistema operativo VMware ESXi 4.1/ESX 4.1, que puede deberse a cualquiera de los siguientes motivos:
  - El modo `Cierre de seguridad` está activado cuando inicia sesión en el servidor o mientras está conectado a Server Administrator. Para obtener más información sobre el modo `Cierre de seguridad`, consulte la documentación de VMware.
  - La contraseña se modifica mientras está conectado a Server Administrator.
  - Usted inicia sesión en Server Administrator como usuario normal, sin privilegios de administrador. Para obtener más información, consulte la documentación de VMware sobre la asignación de la función.

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

Puede corregir una instalación defectuosa si fuerza una reinstalación y luego 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 del sitio web de asistencia de Dell, en **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 **Instalación personalizada** y elija todos los componentes que se instalaron originalmente. Si no tiene certeza sobre cuáles componentes estaban instalados, seleccione todos los componentes y realice la instalación.

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

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

Servicios de OpenManage Server Administrator

Esta tabla muestra los servicios que utiliza Server Administrator para proporcionar información sobre la administración de sistemas y el impacto que provoca la falla de estos servicios.

Tabla A-1. Servicios de OpenManage Server Administrator

Nombre del servicio	Descripción	Impacto de la falla	Mecanismo de recuperación	Gravedad
Windows: DSM SA Servicio de conexión Linux: dsm_om_connsvc (Este servicio se instala con Web Server de Server Administrator).	Brinda acceso local/remoto a Server Administrator desde cualquier sistema con explorador de web compatible y conexión de red.	Los usuarios no pueden iniciar sesión en Server Administrator ni ejecutar operaciones a través de la interfaz web del usuario. No obstante, aún podrá utilizarse la interfaz CLI.	Reiniciar el servicio	Crítico
Servicio común				
Windows: DSM SA compartido Servicios Linux: dsm_om_shrsvc (Este servicio se ejecuta en Managed System.)	Ejecuta el recopilador de 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).	No es posible realizar actualizaciones de software con ITA. Sin embargo, podrán realizarse actualizaciones de forma local y fuera de Server Administrator mediante paquetes individuales Dell Update Package. Las actualizaciones podrán ejecutarse mediante herramientas de terceros (como MSSMS, Altiris y Novell ZENworks).	Reiniciar el servicio	Aviso
NOTA: Si las bibliotecas de compatibilidad de 32 bits no están instaladas en un sistema Linux de 64 bits, los servicios compartidos no pueden iniciar el recopilador de inventarios y muestran el mensaje de error `libstdc++.so.5 is required to run the Inventory Collector (se necesita libstdc++.so.5 para ejecutar el recopilador de inventarios)`. srvadmin-cm.rpm proporciona los binarios para el recopilador de inventarios. Para conocer la lista de RPM de los que depende `srvadmin-cm`, consulte la *Guía de instalación de Dell OpenManage Server Administrator*.				
Servicios de instrumentación				
Windows: Administrador de datos de DSM SA Linux: dsm_sa_datamgrd (como parte del servicio dataeng) (Este servicio se ejecuta en Managed System.)	Supervisa el sistema, ofrece acceso rápido a información detallada sobre fallas y rendimiento, y permite la administración remota de los sistemas supervisados, incluidos el apagado, el inicio y la seguridad.	Los usuarios no pueden configurar/ver los detalles a nivel de hardware en la interfaz gráfica de usuario o la interfaz de línea de comandos sin que estos servicios estén en ejecución.	Reiniciar el servicio	Crítico
Administrador de sucesos de DSM SA (Windows) Linux: dsm_sa_eventmgrd (como parte del servicio dataeng) (Este servicio se ejecuta en Managed System.)	Proporciona el servicio de registro de sucesos de archivos y sistema operativo para la administración de sistemas, y también es usado por analizadores de registros de sucesos.	Si se detiene este servicio, no funcionan correctamente las funciones de registro de sucesos.	Reiniciar el servicio	Aviso
Linux: dsm_sa_snmpd (como parte del servicio dataeng) (Este servicio se ejecuta	Motor de datos SNMP de Linux Interfaz	La solicitud SNMP para obtener/establecer/capturar no funciona desde una estación de administración.	Reiniciar el servicio	Crítico

en Managed System.)				
Servicio de administración de almacenamiento				
Windows: mr2kserv (Este servicio se ejecuta en Managed System.)	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 todos los controladores RAID y no RAID admitidos.	Reiniciar el servicio	Crítico

Regresar a la página de contenido

Regresar a la página de contenido

Preguntas frecuentes

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

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

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

1. **¿Cuáles son las tareas que deben realizarse después de agregar un sistema operativo VMware ESX 4.1 al dominio de Active Directory?**

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

   - Iniciar sesión en Server Administrator mientras se usa el sistema operativo VMware ESX 4.1 como Server Administrator y reiniciar el servicio de conexión de DSM SA.
   - Iniciar sesión en el nodo remoto mientras se usa el sistema operativo VMware ESX 4.1 como agente de Remote Enablement. Esperar aproximadamente 5 minutos hasta que el proceso sfcbd agregue el permiso para el nuevo usuario.

2. **¿Cuál es el nivel de permiso mínimo que necesita un usuario para instalar Server Administrator?**

   Para instalar Server Administrator es necesario contar con permiso de nivel de **Administrador** como mínimo. Los usuarios comunes y usuarios avanzados no están autorizados para instalar Server Administrator.

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

   Para los sistemas que tienen la versión 4.3 de Server Administrator, no se requiere una ruta de actualización. Para los sistemas que tienen una versión anterior a la 4.3, en primer lugar es necesario actualizar a la versión 4.3 y luego a una versión 6.x (la "x" indica la versión de Server Administrator a la que se desea actualizar).

4. **¿Cómo puedo determinar cuál es la versión más reciente de Server Administrator disponible para mi sistema?**

   Acceda a: **support.dell.com→ Enterprise IT (TI para empresas)→ Manuals (Manuales)→ Software→ Systems Management → Dell OpenManage Server Administrator**

   La versión más reciente de documentación indica la versión disponible de OpenManage Server Administrator.

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

   Después de iniciar sesión en Server Administrator, acceda a **Propiedades→ Resumen**. La versión de Server Administrator instalada en el sistema se indica en la columna **Systems Management**.

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

   Sí, el usuario puede definir su puerto https preferido. Para ello, acceda a **Preferencias→ Configuración general→Web Server→Puerto HTTPS**

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

   NOTA: Si se cambia el número de puerto a uno no válido o a un número de puerto en uso, es posible que se impida que otras aplicaciones o exploradores accedan al Server Administrator en el Managed System (sistema administrado). Consulte la *Guía del usuario de instalación y seguridad de Dell OpenManage* para ver la lista de puertos predeterminados.

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

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

8. **¿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.

9. **¿Se requiere SNMP para descubrimiento de ITA, inventario y actualizaciones de software en los sistemas PowerEdge? ¿Puede utilizarse sólo CIM, sin otra ayuda, para descubrimiento, inventario y 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 Dell 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 presupone la existencia de 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. El inventario 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. Luego se invocan funciones de 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 tales como impresoras en red, el estándar sigue siendo SNMP para establecer comunicación con (principalmente descubrir) el dispositivo.

Los dispositivos tales como equipos de almacenamiento EMC cuentan con protocolos patentados. Puede encontrarse información acerca de este entorno en las tablas de puertos utilizados incluidas en la documentación de OpenManage.

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

    No. En esta versión no hay planes referidos a la compatibilidad con SNMP v3.

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

    Sí, el uso de un carácter de guión bajo en el nombre de dominio no es válido. Tampoco son válidos los demás caracteres especiales (a excepción del guión). Use sólo caracteres alfanuméricos que no distingan entre mayúsculas y minúsculas.

12. **¿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 privilegios?**

    Si no selecciona la casilla de Active Directory, sólo contará con el acceso que está configurado en Microsoft Active Directory. No podrá iniciar sesión mediante la solución de esquema extendido de Dell (Dell Extended Schema Solution) en Microsoft Active Directory. Esta solución le permite proporcionar acceso a Server Administrator, con la capacidad de agregar/controlar usuarios y privilegios de Server Administrator para los usuarios ya existentes en el software Active Directory. Para obtener más información, consulte "Uso de Microsoft Active Directory" en la *Guía de instalación de Dell OpenManage Server Administrator*.

13. **¿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, por:

    Para 32-bit:

    ```
    auth required pam_stack.so service=system-auth

    auth required /lib/security/pam_nologin.so

    account required pam_stack.so service=system-auth
    ```

    For 64-bit:

    ```
    auth required pam_stack.so service=system-auth

    auth required /lib64/security/pam_nologin.so

    account required pam_stack.so service=system-auth
    ```

Regresar a la página de contenido

Regresar a la página de contenido

Servicios de Server Administrator

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Descripción general

Dell OpenManage Server Administrator Instrumentation Service supervisa la condición de un sistema y ofrece acceso rápido a la información detallada sobre fallas y rendimiento que se recopila por medio de agentes de administración de sistemas estándar de la industria. Las características de informe y visualización permiten recuperar el estado general de cada chasis que constituye el sistema. En el nivel de subsistemas, puede ver información sobre los voltajes, las temperaturas, las revoluciones por minuto del ventilador y el funcionamiento de la memoria en los puntos clave del sistema. En la vista de resumen, puede ver los detalles de cada costo de propiedad (COO) relevante del sistema. Se puede recuperar fácilmente la información sobre la versión del BIOS, firmware, sistema operativo y de todo el software Systems Management instalado.

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

- Especificar los valores mínimo y máximo para determinados componentes críticos. Los valores, denominados umbrales, determinan el intervalo en el que se produce un suceso de advertencia para ese componente (el fabricante del sistema especifica los valores de falla mínimo y máximo).
- Especificar cómo responde el sistema cuando se produce un suceso de advertencia o de falla. Los usuarios pueden configurar las acciones que realiza un sistema como respuesta a las notificaciones de sucesos de advertencia y falla. Asimismo, los usuarios que tienen supervisión continua pueden especificar que no se debe realizar ninguna acción y confiar en el criterio humano para seleccionar la mejor acción de 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 de protocolo simple de administración de red (SNMP) de manera tal que admita paquetes SNMP tanto para sistemas administrados como para estaciones de administración de red que ejecuten Microsoft Windows Server 2003. Consulte "Configuración del agente SNMP en sistemas que ejecutan sistemas operativos Windows compatibles" para obtener más detalles.

Administración del sistema

La página de inicio de Server Administrator toma como predeterminado el objeto **Sistema** de la vista de árbol del sistema. El valor predeterminado para el objeto **Sistema** abre los componentes de **Estado** en la ficha **Propiedades**.

La página de inicio de **Preferencias** muestra de manera predeterminada la ventana **Configuración de acceso** en la ficha **Preferencias**.

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

NOTA: La ayuda contextual en línea está disponible para cada ventana de la página de inicio de Server Administrator. Al hacer clic en **Ayuda** en la barra de navegación global, se abre una ventana de ayuda independiente que contiene información detallada sobre la ventana específica que se está viendo. La ayuda en línea está diseñada para guiarlo por las acciones específicas necesarias para llevar a cabo todos las tareas relacionadas con los servicios de Server Administrator. La ayuda en línea está disponible para todas las ventanas que se pueden ver, organizada de acuerdo con los grupos de software y hardware que Server Administrator descubre en el sistema y con el nivel de privilegios del usuario.

NOTA: Debe tener privilegios de usuario avanzado o administrador para ver muchos de los objetos de árbol del sistema, componentes del sistema, fichas de acción y características de área de datos que se pueden configurar. Además, sólo los usuarios conectados con privilegios de administrador pueden acceder a las funciones críticas del sistema, como la función de apagado que se incluye en la ficha **Apagado**.

Administración de objetos de árbol de módulos de servidor o sistema

El árbol de módulos de servidor o sistema de Server Administrator muestra todos los objetos del sistema visibles de acuerdo con los grupos de software y hardware que Server Administrator descubre en Managed System y con los privilegios de acceso del usuario. Los componentes del sistema se clasifican según el tipo del componente. Al ampliar el objeto principal -"**Gabinete modular**"-"**Módulo de servidor o sistema**"**-** pueden aparecer las categorías principales de los componentes del sistema: "**Chasis del sistema principal / Sistema principal**", "**Software**" y "**Almacenamiento**".

Si Storage Management Service está instalado, de acuerdo con el controlador y almacenamiento conectados al sistema, el objeto de árbol de almacenamiento se expande para mostrar varios objetos.

Para obtener información detallada sobre el componente Storage Management Service, consulte la *Guía del usuario de Dell OpenManage Server Administrator Storage Management* que se encuentra en el sitio web de asistencia de Dell en **support.dell.com / manuals**.

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

Funciones no admitidas en OpenManage Server Administrator

Debido a las limitaciones de las versiones 4.X del sistema operativo VMware ESXi, algunas funciones disponibles en versiones anteriores de OpenManage Server Administrator no se encuentran disponibles en esta versión, a saber:

Funciones no admitidas en ESXi 4.X

- Administración de alertas: Acciones de alerta
- Interfaz de red: Estado administrativo
- Interfaz de red: DMA
- Interfaz de red: Dirección de protocolo de Internet (IP)
- Interfaz de red: Unidad máxima de transferencia
- Interfaz de red: Estado operativo
- Preferencias: Configuración de SNMP
- Apagado remoto: Ciclo de encendido del sistema con apagado de sistema operativo en primer lugar
- Acerca de los detalles: Los detalles del componente Server Administrator no están enumerados en la ficha Detalles
- Mapa de funciones

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

NOTA: Los privilegios de usuario avanzado o administrador son necesarios para ver muchos de los objetos de árbol del sistema, componentes del sistema, fichas de acción y características de área de datos que se pueden configurar. Además, sólo los usuarios conectados con privilegios de administrador pueden acceder a las funciones críticas del sistema, como es la función de apagado que se incluye en la ficha **Apagado**.

Gabinete modular

NOTA: Para los fines de Server Administrator, *gabinete modular* se refiere a un sistema que puede tener uno o más sistemas modulares que aparecen como un módulo de servidor independiente en el árbol del sistema. Como un módulo de servidor independiente, el gabinete modular contiene todos los componentes esenciales de un sistema. La única diferencia es que hay ranuras para dos módulos de servidor como mínimo dentro de un contenedor más grande y cada uno de ellos es un sistema tan completo como un módulo 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**.

Propiedades

Subfichas: Información

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

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

Acceso y uso de Chassis Management Controller

Para acceder a la ventana **Inicio de sesión** de Chassis Management Controller desde la página principal de Server Administrator:

1. Haga clic en el objeto **Gabinete modular**
2. Haga clic en la ficha **Información de CMC** y luego en **Abrir la interfaz web de CMC**. Aparecerá la página **Inicio de sesión** de CMC.

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

Módulo de servidor o sistema

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

Propiedades

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

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

- Ver la condición de alerta del estado 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 está supervisando.

- Ver y configurar la información de propiedad del sistema que se está supervisando.
- Ver y establecer las acciones de recuperación automática del sistema (el temporizador de vigilancia del sistema operativo) del sistema que se supervisa.

NOTA: Es posible que las opciones de recuperación automática del sistema no estén disponibles debido a que el temporizador de vigilancia del sistema operativo está activado en el BIOS. Para configurar las opciones de recuperación automática, el temporizador de vigilancia del sistema operativo deberá estar desactivado.

NOTA: Es posible que las acciones de recuperación automática del sistema no se ejecuten exactamente durante el periodo de tiempo de espera establecido (n segundos) cuando la vigilancia identifique un sistema que ha dejado de responder. El tiempo de ejecución de la acción varía de *n-h+1* a *n+1* segundos, donde *n* es periodo de tiempo de espera establecido y *h* es el intervalo de latido. El valor del intervalo de latido es de 7 segundos cuando $n \leq 30$ y de 15 segundos cuando $n > 30$.

NOTA: La funcionalidad de la característica de temporizador de vigilancia no se puede garantizar cuando se presente un suceso de memoria no corregible en el DRAM Bank_1 del sistema. Si en esta ubicación se presenta un suceso de memoria no corregible, es posible que se dañe el código del BIOS que reside en este espacio. Como la función de vigilancia utiliza un comando de BIOS para efectuar el apagado o el reinicio, es posible que ésta no funcione correctamente. Si esto ocurre, se deberá reiniciar manualmente el sistema.

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 falla.

NOTA: Un apagado térmico sólo se presentará cuando la temperatura que el sensor informa supere el umbral de temperatura. Un apagado térmico no se presentará cuando la temperatura que el sensor informa esté por debajo del umbral de temperatura.

- Apague el servicio de conexión de DSM SA (Web Server).

NOTA: Server Administrator aún está disponible mediante la interfaz de línea de comandos (CLI) cuando el servicio de conexión de DSM SA está apagado. Las funciones de la CLI no requieren que el servicio de conexión DSM SA esté funcionando.

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 indicador de estado que se encuentra junto al nombre del registro cambia de estado normal ( ) a estado no crítico ( ) cuando el archivo de registro alcanza el 80% de su capacidad. En los sistemas Dell PowerEdge *x8xx*, *x9xx y xx1x*, el icono indicador de estado que se encuentra junto al nombre del registro cambia al estado crítico ( ) cuando el archivo de registro alcanza el 100% de su capacidad.

NOTA: Se recomienda que borre el registro de hardware cuando alcance el 80% de la capacidad. Si se permite que el registro llegue al 100% de la capacidad, los sucesos más recientes se eliminarán 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: Consulte la *Guía de referencia de mensajes de Server Administrator* para obtener una explicación completa de la descripción, el nivel de gravedad y la causa de todas las identificaciones de sucesos de alerta.

- 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: Consulte "Registros de Server Administrator" para obtener instrucciones completas sobre visualización, impresión, almacenamiento y envío por correo electrónico de registros.

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 falla.
- Ver los valores actuales de los filtros de sucesos de plataforma y establecer las acciones de filtración de sucesos de plataforma que se deberán realizar en caso de que el sensor de un componente del sistema devuelva un valor de advertencia o de falla. También puede utilizar la opción **Configurar destino** para seleccionar un destino (dirección IPv4 o IPv6) al que se enviará una alerta para un suceso de plataforma.

NOTA: Server Administrator no muestra la identificación de alcance de la dirección IPv6 en la interfaz gráfica de usuario.

- Ver los umbrales actuales de alerta de las capturas SNMP y establecer los niveles de umbral de alerta para los componentes del sistema instrumentado. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

NOTA: Las acciones de alerta para todos los sensores potenciales de componentes del sistema se enumeran en la ventana **Acciones de alerta**, incluso si no están presentes en su sistema. Ajustar acciones de alerta para sensores de componentes del sistema que no existen en el sistema no tendrá efecto.

Administración de sesiones

Subfichas: Sesión

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

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

NOTA: Solamente los usuarios con privilegios administrativos pueden ver la página Administración de sesiones y terminar las sesiones de 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 del hardware
- Intromisión
- Memoria
- Red
- Puertos
- Administración de la alimentación
- Suministros de energía
- Procesadores
- Acceso remoto
- Unidades flash extraíbles
- Ranuras
- Temperaturas
- Voltajes

NOTA: Rendimiento del hardware, que sólo se admite en los sistemas Dell *xx0x* y posteriores.
Suministros de energía, un componente que no está disponible en los sistemas Dell PowerEdge 1900.
Administración de la alimentación, que sólo se admite en ciertos sistemas Dell *xx0x* y posteriores.

El módulo de servidor o sistema puede tener un chasis de sistema principal o varios. El chasis de sistema principal/sistema principal contiene los componentes esenciales de un sistema. La ventana de acción del objeto **Chasis del sistema principal/Sistema principal** contiene la siguiente ficha: **Propiedades**.

Propiedades

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

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

- Ver la condición o estado de los sensores y de los componentes de hardware. Cada componente de la lista tiene el icono "Indicadores de estado de los componentes del módulo del sistema o servidor" junto a su nombre. Una marca de verificación verde ( ) indica que el componente se encuentra en una condición satisfactoria (normal). Un triángulo amarillo con un signo de admiración dentro ( ) indica que un componente está en una condición de advertencia (no crítica) y requiere atención rápida. Una X roja ( ) indica que el componente está en una condición de falla (crítica) y requiere atención inmediata. Un espacio en blanco ( ) indica que la condición de un componente es desconocida. Entre los componentes supervisados disponibles se incluyen:
  - Baterías
  - Ventiladores
  - Registro de hardware
  - Intromisión
  - Memoria
  - Red

- Administración de la alimentación
- Suministros de energía
- Procesadores
- Temperaturas
- Voltajes

NOTA: Baterías, que sólo se admiten en los sistemas Dell PowerEdge *x9xx* y Dell *xx0x*.
Suministros de energía, un componente que no está disponible en los sistemas Dell PowerEdge 1900.
Administración de la alimentación, que sólo se admite en ciertos sistemas Dell *xx0x* y posteriores.

- Ver información sobre los atributos del chasis del sistema principal.
- Ver información detallada sobre las unidades reemplazables en el campo (FRU) que están instaladas en el sistema (bajo la subficha **Componentes del sistema (FRU)**).
- Activar o desactivar los botones del panel anterior de Managed System, es decir, el botón de encendido y el botón de interrupción no enmascaradora (NMI) (si están presentes en el sistema). Asimismo, seleccionar el nivel de acceso de seguridad de LCD del Managed System (sistema administrado). Es posible seleccionar la información de LCD del Managed System desde el menú desplegable. También es posible activar la indicación de sesión de KVM remoto en la subficha **Panel anterior**.

Baterías

Haga clic en el objeto **Baterías** para ver información sobre las baterías instaladas del sistema. Las baterías mantienen la fecha y hora cuando su sistema está apagado. La batería guarda los valores de configuración del BIOS del sistema, lo que hace posible que el sistema se reinicie con eficiencia. La ventana de acciones del objeto **Baterías** puede tener las siguientes fichas, en función de 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 quiera que se activen en caso de una advertencia de batería o un suceso crítico/falla.

BIOS

Haga clic en el objeto **BIOS** para administrar las funciones claves del BIOS del sistema. El BIOS del sistema contiene programas almacenados en un conjunto de chips de memoria flash que controlan las comunicaciones entre el microprocesador y los dispositivos periféricos, como el teclado y el adaptador de video, y otras funciones diversas, como mensajes del sistema. La ventana de acciones del objeto **BIOS** puede incluir las siguientes fichas, en función de 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

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

Puede modificar el estado de muchas funciones de configuración del BIOS, entre otras, el puerto serie, las tarjetas controladoras de interfaces de red, la secuencia de inicio, la secuencia de unidad de disco duro, los puertos USB para acceso del usuario, la tecnología de virtualización de la CPU, la tecnología HyperThreading de la CPU, el modo de recuperación de corriente alterna, el controlador SATA incorporado, la redirección de consola y velocidad en baudios libre de fallas de la redirección de consola. También puede configurar el dispositivo USB interno, los valores del controlador de unidad óptica, el temporizador de vigilancia de la recuperación de sistema automática (ASR), el hipervisor incorporado y la información de los puertos adicionales de red LAN en la placa base. Puede ver los valores del módulo de plataforma segura (TPM) y del módulo criptográfico seguro (TCM).

Posiblemente se muestren otras características de configuración, dependiendo de la configuración específica de su sistema. Sin embargo, es posible que en la pantalla de configuración mediante F2 del BIOS se muestren algunas opciones de configuración del BIOS a las cuales no se puede acceder desde Server Administrator.

NOTA: La información de configuración del NIC dentro de la configuración del **BIOS** de Server Administrator puede no ser correcta para los NIC incorporados. El uso de la pantalla de configuración del **BIOS** para activar o desactivar los NIC puede producir resultados inesperados. Se recomienda que realice todas las configuraciones de los NIC incorporados por medio de la pantalla **Configuración del sistema** que está disponible al presionar <F2> durante el inicio del sistema.

NOTA: La ficha Configuración del BIOS de su sistema sólo muestra las características del BIOS admitidas en su sistema.

Ventiladores

Al hacer clic en el objeto **Ventiladores**, puede administrar los ventiladores del sistema. Server Administrator supervisa el estado de cada ventilador del sistema midiendo sus rpm. Las sondas de ventilador generan informes sobre las revoluciones por minuto para 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 acciones del objeto **Ventiladores** puede tener las siguientes fichas, en función de 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 cambian de acuerdo con el tipo de firmware que tenga su sistema: BMC o ESM. Algunos valores de umbral no se pueden editar en sistemas basados en BMC.

- Seleccionar las opciones de control del ventilador.

Administración de alertas

Subfichas: Acciones de alerta | **Capturas SNMP**

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

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que un ventilador devuelva un valor de advertencia o de falla.
- Ver los umbrales actuales de alerta de las capturas SNMP y establecer los niveles de los umbrales de alerta para los ventiladores. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

Firmware

Haga clic en el objeto **Firmware** para administrar el firmware del sistema. El firmware está formado por programas o datos que se han escrito en la ROM. El firmware puede iniciar y hacer funcionar un dispositivo. Cada controlador contiene firmware que sirve de ayuda para proporcionar la funcionalidad del controlador. La ventana de acción del objeto **Firmware** puede incluir la siguiente ficha, en función de 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 de rendimiento del sistema. La ventana de acción del objeto **Rendimiento del hardware** puede tener la siguiente ficha, en función de los privilegios de grupo del usuario: **Propiedades**.

Tabla 4-1 muestra una lista de los posibles valores para el estado y causa de una sonda:

Tabla 4-1. 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/D]

Propiedades

Subficha: Información

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

Intromisión

Haga clic en el objeto **Intromisión** para administrar el estado de intromisión al chasis del sistema. Server Administrator supervisa el estado de intromisión al chasis como medida de seguridad para evitar accesos no autorizados a los componentes críticos del sistema. La intromisión al chasis indica que alguien está abriendo o ha abierto la cubierta del chasis del sistema. La ventana de acciones del objeto **Intromisión** puede tener las siguientes fichas, en función de 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 falla.
- Ver los umbrales actuales de alerta de las capturas SNMP y establecer los niveles de los umbrales de alerta para el sensor de intromisión. Las capturas seleccionadas se desencadenan si el sistema genera el 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 de cada módulo de memoria presente en el sistema supervisado. Los sensores previos de falla del dispositivo de memoria supervisan los módulos de memoria por recuento del número de correcciones de memoria de ECC. Server Administrator también supervisa la información de redundancia de memoria si el sistema admite esta función. La ventana de acciones del objeto **Memoria** puede tener las siguientes fichas, en función de los privilegios de grupo del usuario: **Propiedades y Administración de alertas**.

Propiedades

Subficha: Memoria

En la ficha **Propiedades**, puede ver los atributos de la memoria, así como los detalles y el estado de los dispositivos de memoria.

NOTA: Si un sistema que tiene bancos de memoria de repuesto entra en un estado de redundancia perdida, es posible que no pueda determinarse con claridad cuál es el módulo de memoria que lo ha ocasionado. Si no puede determinar cuál es el DIMM que se debe sustituir, consulte la anotación de registro *se detectó un cambio al banco de memoria de repuesto* del registro ESM del sistema para averiguar cuál es el módulo de memoria que falló.

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 falla.
- Ver los umbrales actuales de alerta de las capturas SNMP y establecer los niveles de los umbrales de alerta para los módulos de memoria. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

Red

Haga clic en el objeto **Red** para administrar los NIC del sistema. Server Administrator supervisa el estado de cada NIC presente en el sistema para garantizar una conexión remota continua. Dell OpenManage Server Administrator informa los detalles de la formación de equipos de NIC si ya está configurado en el sistema. Es posible agrupar dos o más NIC físicos en un único NIC lógico al que un administrador puede asignar una dirección IP. La formación de equipos puede configurarse con herramientas de proveedores de NIC. Por ejemplo, Broadcom - BACS. Si falla uno de los NIC físicos, aún es posible acceder a la dirección IP debido a que está vinculada al NIC lógico y no a un único NIC físico. Si se configura la interfaz de equipo, se muestran las propiedades detalladas del equipo. También se informa la relación entre los NIC físicos y la interfaz de equipo y viceversa, si estos NIC físicos son miembros de la interfaz de equipo. La ventana de acción 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 físico y también sobre las interfaces de equipo instaladas en el sistema.

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

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

Propiedades

Subficha: Información

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

Administración de la alimentación

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=watt 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.

También es posible ver la capacidad instantánea del sistema y la capacidad pico del sistema. Los valores se muestran en vatios y BTU/h (unidad térmica británica). Los umbrales de alimentación pueden establecerse en vatios y BTU/h.

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

Administración

Subfichas: Presupuesto | Perfiles

La ficha Presupuesto le permite ver los atributos de inventario de la alimentación, como la alimentación en estado inactivo o la alimentación potencial máxima del sistema, expresados en vatios y BTU/h. También es posible utilizar la opción Presupuesto de alimentación para activar un límite de alimentación y establecerlo 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 sólo estén disponibles en los sistemas activados con el Bus de administración de la alimentación (Power Management Bus, 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 funcione correctamente. La ventana de acciones del objeto Suministros de energía puede incluir las siguientes fichas de acuerdo con los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

Subficha: Elementos

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

- Ver información sobre los atributos de redundancia de los suministros de energía.
- Verificar el estado de cada elemento de suministros de energía, incluso la potencia de entrada nominal y la potencia máxima de salida. El atributo Potencia de entrada nominal sólo se muestra en los sistemas PMBus a partir de *xx1x*.

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 falla.
- Configurar destinos de alertas de sucesos de plataforma para direcciones IPv6.
- Ver los umbrales actuales de alerta de las capturas SNMP y establecer los niveles de umbral de alerta para la potencia del sistema expresada en vatios. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

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

Procesadores

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

Subficha: Información

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 alerta | **Capturas SNMP**

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 falla.
- Ver los umbrales de alerta actuales de las capturas SNMP y establecer los niveles de los umbrales de alerta para los procesadores. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

Acceso remoto

Haga clic en el objeto **Acceso remoto** para administrar las funciones del Controlador 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, puede administrar funciones del BMC/iDRAC, como la información general sobre el BMC o sobre el iDRAC. También puede administrar la configuración del BMC/iDRAC en una red de área local (LAN), el puerto serie del BMC/iDRAC, la configuración del modo de terminal del puerto serie, el BMC/iDRAC de una comunicación en serie en la LAN y los usuarios del BMC/iDRAC.

NOTA: El BMC se admite en los sistemas Dell PowerEdge *x8xx* y *x9xx*, mientras que el iDRAC sólo se admite en los sistemas Dell *xx0x* y *xx1x*.

NOTA: Si utiliza una aplicación que no sea Server Administrator para configurar el BMC/iDRAC mientras Server Administrator se está ejecutando, es posible que se produzca una asincronía entre los datos de configuración del BMC/iDRAC mostrados por Server Administrator y el BMC/iDRAC. Se recomienda utilizar Server Administrator para configurar el BMC/iDRAC si Server Administrator se está ejecutando.

El DRAC le permite tener acceso a las funciones de administración remota de su sistema. El DRAC de Server Administrator proporciona el acceso remoto a sistemas no operativos, notificación de alertas cuando se apaga un sistema y la posibilidad de reiniciar un sistema.

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

Propiedades

Subficha: Información

La ficha **Propiedades** le permite ver información general sobre el dispositivo de acceso remoto. También le permite ver los atributos de las direcciones IPv4 e IPv6.

Haga clic en **Restablecer valores predeterminados** para restablecer todos valores predeterminados de los atributos en el sistema.

Configuración

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

En la ficha **Configuración**, cuando el BMC/iDRAC está configurado, puede configurar el BMC/iDRAC en una LAN, el puerto serie para el BMC/iDRAC y el BMC/iDRAC de una comunicación en serie en la LAN.

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

Cuando el DRAC está configurado, la ficha **Configuración** le permite:

Configurar propiedades de red

NOTA: Los campos **Activar el NIC**, **Selección del NIC** y **Clave de cifrado** sólo se muestran en los sistemas Dell PowerEdge *x9xx*.

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

NOTA: La activación o desactivación de IPv4/IPv6 sólo 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 acerca de los usuarios del Remote Access Controller.

NOTA: En los sistemas Dell PowerEdge *x9xx*:
- Se muestran diez identificaciones de usuario. Si hay una tarjeta DRAC instalada, se mostrarán dieciséis identificaciones de usuario.
- Se muestra la columna Carga de comunicación en serie en la LAN.

Unidades flash extraíbles

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

Propiedades

Subficha: Información

En la ficha **Propiedades** se puede ver la información acerca de las unidades flash extraíbles y los módulos SD internos. Esto incluye la información sobre el nombre del conector, su estado y la capacidad de almacenamiento.

Administración de alertas

Subfichas: Acciones de alerta | **Capturas SNMP**

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

- Ver los valores actuales de las acciones de alerta y establecer las acciones de alerta que desea que se realicen en caso de que la sonda de unidades flash extraíbles devuelva un valor de advertencia o de falla.
- Ver los umbrales de alerta actuales de las capturas SNMP y establecer los niveles de los umbrales de alerta para las sondas de unidades flash

extraíbles. Las capturas seleccionadas se desencadenan si el sistema genera el suceso correspondiente en el nivel de gravedad seleccionado.

La administración de alertas es común a los módulos SD internos y vFlash. Al configurar las acciones de alerta/SNMP/PEF ya sea para los módulos SD o para vFlash, se configuran automáticamente para el otro.

Ranuras

Haga clic en el objeto **Ranuras** para administrar los conectores o los zócalos de la placa base que aceptan tarjetas de circuitos impresos, como las tarjetas de expansión. La ventana de acción 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. Server Administrator supervisa la temperatura en varias ubicaciones del chasis del sistema para garantizar que la temperatura del interior del chasis no suba demasiado. La ventana de acciones del objeto **Temperaturas** muestra las siguientes fichas, en función de los privilegios de grupo del usuario: **Propiedades** y **Administración de alertas**.

Propiedades

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 la sonda de temperatura cambian de acuerdo con el tipo de firmware que tenga su sistema: BMC o ESM. Algunos valores de umbral no se pueden editar en sistemas basados en BMC. Al asignar valores de umbrales de sonda, Server Administrator a veces redondea los valores mínimos o máximos introducidos al valor asignable más cercano.

Administración de alertas

Subfichas: Acciones de alerta | **Capturas SNMP**

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

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

NOTA: Puede establecer los valores máximos y mínimos para los umbrales de la sonda de temperatura de un chasis externo sólo con números enteros. Si intenta establecer un valor para el umbral mínimo o máximo de la sonda de temperatura con un número que contenga decimales, únicamente el número entero antes de la posición decimal se guardará como el valor del umbral.

Voltajes

Al hacer clic en el objeto **Voltajes**, puede administrar los niveles de voltaje en el sistema. Server Administrator supervisa los voltajes de los componentes críticos en distintas ubicaciones de chasis del sistema supervisado. La ventana de acciones del objeto **Voltajes** puede tener las siguientes fichas, en función de 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 sonda de voltaje.

NOTA: Algunos campos de la sonda de voltaje cambian de acuerdo con el tipo de firmware que tenga su sistema: 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 falla.
- Ver los umbrales actuales de las alertas 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 el suceso correspondiente en el nivel de gravedad seleccionado.

Software

Haga clic en el objeto **Software** para ver información detallada sobre la versión de los componentes de software esenciales de Managed System, por ejemplo, el sistema operativo y el software Systems Management. La ventana de acción del objeto **Software** tiene la siguiente ficha, en función de los privilegios de grupo del usuario: **Propiedades**.

Propiedades

Subficha: Resumen

En la ficha **Propiedades**, puede ver un resumen del software del sistema operativo del sistema supervisado y del software System Management.

Sistema operativo

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

Propiedades

Subficha: Información

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

Almacenamiento

Server Administrator proporciona el Storage Management Service:

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

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

En el caso de Storage Management Service, la ventana de acción 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 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 mostradas se basan en el software Systems Management instalado en Managed System.

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

- 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 seleccionadas de Server Administrator. La ventana de acción del objeto **Configuración general** incluye las siguientes fichas, en función de los privilegios de grupo del usuario: **Usuario** y **Web Server**.

Usuario

Subficha: Propiedades

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. Consulte "Servicio de conexión y configuración de seguridad de la administración de servidores de Dell Systems Management" para obtener instrucciones acerca de cómo configurar las preferencias del servidor.
- Configurar la dirección de servidor SMTP y la dirección IP de enlace ya sea en el modo de dirección IPv4 o IPv6.
- Llevar a cabo la administración de certificados X.509 al generar un nuevo certificado X.509, volver a usar un certificado X.509 o importar un certificado raíz o cadena de certificados de una autoridad de certificación (CA). Para obtener más información sobre 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 los usuarios con privilegios de usuario o de usuario avanzado y configurar la contraseña root de SNMP. La ventana de acción del objeto **Server Administrator** puede incluir la siguiente ficha, en función de los privilegios de grupo del usuario: **Preferencias**.

Preferencias

Subficha: Configuración de acceso | Configuración de SNMP

En la ficha **Preferencias**, puede:

- Activar o desactivar el acceso de usuarios con privilegios de usuario o de usuario avanzado.
- Configurar la contraseña root de SNMP.

  NOTA: El usuario predeterminado para la configuración SNMP es `root` y la contraseña es `calvin`.

- Configurar las operaciones Set de SNMP.

  NOTA: Después de configurar las operaciones Set de SNMP, se deben reiniciar los servicios para que los cambios tengan efecto. En sistemas que ejecutan sistemas operativos Microsoft Windows admitidos, se debe reiniciar el servicio SNMP de Windows. En sistemas que ejecutan sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server admitidos, se deben reiniciar los servicios de Server Administrator ejecutando el comando de reinicio `srvadmin-services.sh`.

Regresar a la página de contenido

Regresar a la página de contenido

Introducción

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Información general

Dell OpenManage Server Administrator (OMSA) ofrece una solución integral de administración de sistemas individualizada mediante dos opciones: una interfaz gráfica de usuario (GUI) integrada a la que se puede acceder mediante explorador web y una interfaz de línea de comandos (CLI) a través del sistema operativo. Server Administrator ha sido diseñado para que los administradores de sistemas los administren de forma local o remota en una red. Se trata de una solución que les permite a los administradores de sistemas centrarse en la administración de toda la red, al ofrecer administración completa de sistemas individualizada.

En el contexto de Server Administrator, un sistema puede ser un sistema independiente, un sistema con unidades de almacenamiento en red conectadas en un chasis separado o un sistema modular compuesto por uno o más 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 permite administrar y dar mantenimiento con facilidad a sistemas locales y remotos mediante un conjunto completo de servicios de administración integrados. Server Administrator es la instalación única en el sistema que se está administrando y se puede acceder a él tanto de forma local como remota desde la página de inicio de **Server Administrator**. Se puede acceder a los sistemas supervisados de forma remota a través de conexiones inalámbricas, de LAN o de marcación de línea directa. Server Administrator garantiza la seguridad de las conexiones de administración mediante el control de acceso basado en funciones (RBAC), la autentificación y el cifrado de capa de sockets seguros (SSL).

Instalación

Puede instalar Server Administrator por medio del *DVD Dell Systems Management Tools and Documentation*. El DVD ofrece un programa de configuración para instalar, actualizar y desinstalar los componentes de Server Administrator, de Managed System y de Management Station Software. Server Administrator también se puede instalar en varios sistemas de una red mediante una instalación desatendida.

El instalador de Dell OpenManage proporciona secuencias de comandos de instalación y paquetes RPM para instalar y desinstalar Dell OpenManage Server Administrator y otros componentes del software Managed System en el sistema administrado. Para obtener más información, consulte la *Guía de instalación de Dell OpenManage Server Administrator y la Guía de instalación de Dell OpenManage Management Station Software*. Puede acceder a estos documentos en el sitio web de asistencia de Dell en **support.dell.com / manuals.**

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

Actualización de los componentes individuales del sistema

Para actualizar componentes individuales del sistema, utilice los Dell Update Packages específicos para los componentes. Utilice el *DVD Dell Server Updates* para ver el informe completo de versiones y actualizar todo un sistema. Server Update Utility es una aplicación basada en DVD-ROM que permite identificar y aplicar actualizaciones en el sistema. La utilidad Server Update Utility se puede descargar del sitio **support.dell.com**.

Consulte la *Guía del usuario de Server Update Utility* para más 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 de la lista del repositorio.

Storage Management Service

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

Para obtener información detallada sobre Storage Management Service, consulte la *Guía del usuario de Dell OpenManage Server Administrator Storage Management* que se encuentra en el sitio web de asistencia de Dell en **(support.dell.com / manuals**).

Instrumentation Service

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

Remote Access Controller

Remote Access Controller ofrece una solución integral de administración remota para los sistemas que cuentan con Dell Remote Access Controller (DRAC) o el controlador de administración de la placa base (BMC)/Integrated Dell Remote Access Controller (iDRAC). Remote Access Controller proporciona acceso remoto a un sistema inoperable, permitiéndole recuperarlo y hacerlo funcionar de la manera más rápida posible. Remote Access Controller también ofrece notificaciones de alerta cuando un sistema está apagado y permite reiniciar un sistema de forma remota. Además, Remote Access Controller registra la causa probable de los bloqueos del sistema y guarda la pantalla de bloqueo más reciente.

Registros

Server Administrator muestra registros de comandos emitidos hacia el sistema o por el mismo, sucesos de hardware supervisados y alertas del sistema. Los registros se pueden ver en la página de inicio, imprimir o guardar como informes y enviarse por correo electrónico a un contacto de servicio designado.

Novedades de la versión 6.3

A continuación se describen las principales características de OpenManage Server Administrator 6.3:

- Se agregó compatibilidad con los siguientes sistemas operativos:
  - VMware ESX 4.0 U1 y 4.1 (compatibilidad sólo con la consola de servicio)
  - VMware ESXi 4.0 U1 y 4.1
  - Citrix XenServer 5.6
  - Red Hat Enterprise Linux versión 5.5 y sistemas EM64T
  - Novell SLES v11 SP1 en sistemas EM64T (en modo XEN, compatibilidad sólo con la consola de servicio)
- Se actualizó Java Runtime Environment (JRE) a la versión 1.6.0 17
- Se agregó compatibilidad con el testigo de BIOS del módulo criptográfico seguro (TCM)
- Se admiten sistemas operativos de 64 bits
- Se admite Server Administrator con exploración por fichas
- Se descartaron los siguientes sistemas operativos:
  - Red Hat Enterprise Linux versión 5.3
  - VMware ESX 3.5 y 4.0
  - VMware ESXi 3.5 y 4.0

Para ver una lista de sistemas operativos admitidos, consulte la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra en el sitio web de asistencia de Dell en **support.dell.com/manuals**.

Consulte la ayuda contextual en línea de Server Administrator para obtener más información sobre las nuevas funciones que presenta esta versión.

Disponibilidad de estándares de administración de sistemas

Dell OpenManage Server Administrator admite los siguientes protocolos principales de administración de sistemas:

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

Si su sistema es compatible con SNMP, debe instalar y habilitar el servicio en el sistema operativo. Si los servicios SNMP están disponibles en el sistema operativo, el programa de instalación de Server Administrator instalará los agentes de asistencia para SNMP.

Todos los sistemas operativos son compatibles con HTTPS. La compatibilidad con CIM y SNMP depende del sistema operativo y, en algunos casos, de la versión del sistema operativo.

Para obtener información sobre cuestiones de seguridad de SNMP, consulte el archivo **léame** de Dell OpenManage Server Administrator (incluido en la aplicación Server Administrator) o el sitio web de asistencia de Dell en **support.dell.com/manuals**. Debe aplicar actualizaciones de los agentes SNMP maestros de su sistema operativo para garantizar que los subagentes SNMP de Dell sean seguros.

Disponibilidad en sistemas operativos compatibles

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

Server Administrator aporta un nivel de seguridad importante a estos estándares de administración de sistemas. Todas las operaciones de definición de atributos (por ejemplo, el cambio de valor de una etiqueta de propiedad) deben llevarse a cabo con Dell OpenManage IT Assistant mientras se mantiene una sesión con la autorización requerida.

La Tabla 1-1 muestra los estándares de administración de sistemas disponibles para cada sistema operativo compatible.

Tabla 1-1. 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 captura de SNMP **NOTA:** Si bien ESXi admite capturas SNMP, no es compatible con el inventario de hardware a través de SNMP.	Disponible
Citrix XenServer 5.6.	Disponible en el paquete **net-snmp** desde el medio de instalación del sistema operativo	No disponible

Página de inicio de Server Administrator

La página de inicio de **Server Administrator** proporciona tareas de administración de sistemas basadas en explorador web fáciles de instalar y de usar, desde el Managed System o desde un host remoto mediante una red LAN, un servicio dial-up o una red inalámbrica. Cuando el servicio de conexión Dell Systems Management Server Administrator (servicio de conexión DSM SA) está instalado y configurado en el Managed System, se pueden realizar funciones de administración remotas desde cualquier sistema que tenga una conexión y un explorador de web compatibles. Además, la página de inicio de **Server Administrator** ofrece una amplia ayuda contextual en línea.

Otros documentos útiles

Además de esta guía, es posible acceder a las siguientes guías en el sitio web de asistencia de Dell: **support.dell.com/manuals**. En la página **Manuals (Manuales)**, haga clic en **Software→ Systems Management**. Haga clic en el vínculo del producto correspondiente que se encuentra a la derecha para tener acceso a los documentos.

- La *Matriz de compatibilidad de software de sistemas Dell* ofrece información sobre los diversos sistemas Dell, los sistemas operativos compatibles con esos sistemas y los componentes de Dell OpenManage que se pueden instalar en estos sistemas.
- La *Guía de instalación de Dell OpenManage Server Administrator contiene instrucciones para ayudar a instalar Dell OpenManage Server Administrator*.
- La *Guía de instalación de Dell OpenManage Management Station Software contiene instrucciones para ayudar a instalar este software que incluye la utilidad de administración de la placa base, DRAC Tools y Active Directory Snap-In*.
- La *Guía de referencia de SNMP de Dell OpenManage* Server Administrator documenta la base de información de administración (MIB) del protocolo de administración de red sencillo (SNMP). MIB de SNMP define variables que extienden la MIB estándar para abarcar las capacidades de los agentes de administración de sistemas.
- La *Guía de referencia del CIM de Dell OpenManage* Server Administrator documenta el proveedor del Modelo común de información (CIM), una extensión del archivo de formato de objeto de administración (MOF) estándar. El archivo MOF del proveedor de CIM describe las clases de objetos de administración compatibles.
- En la *Guía de referencia de mensajes de Dell OpenManage Server Administrator* 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. En esta guía se explica el texto, la gravedad y la causa de cada uno de los mensajes de alerta de Instrumentation Service que envía Server Administrator.
- La *Guía del usuario de la interfaz de línea de comandos de Dell OpenManage* Server Administrator documenta la interfaz de línea de comandos de Server Administrator completa, incluyendo una explicación de los comandos de la CLI para ver el estado del sistema, acceder a registros, crear informes, configurar diversos parámetros de componentes y establecer umbrales de falla.
- La *Guía del usuario de Integrated Dell Remote Access Controller* proporciona información detallada sobre la configuración y el uso del iDRAC.
- La *Guía del usuario de Dell Chassis Management Controller* proporciona información detallada sobre la instalación, la configuración y el uso de CMC.
- La *Guía del usuario de Dell Online Diagnostics* contiene información completa sobre cómo instalar y usar Online Diagnostics en el sistema.
- La *Guía del usuario de las utilidades del controlador de administración de la placa base Dell OpenManage* proporciona información adicional sobre cómo usar Server Administrator para configurar y administrar el BMC del sistema.
- La *Guía del usuario de Dell OpenManage Server Administrator Storage Management* es una guía de referencia completa para la configuración y administración del almacenamiento local y remoto conectado a un sistema.
- La *Guía del usuario Racadm de Dell* Remote Access Controller proporciona información sobre el uso de la utilidad de línea de comandos racadm.
- La *Guía del usuario de Dell* Remote Access Controller 5 proporciona información completa sobre cómo instalar y configurar un controlador DRAC 5, y cómo usar DRAC 5 para acceder de manera remota a un sistema que no funciona.
- La *Guía del usuario de los Dell Update Packages* proporciona información acerca de cómo obtener y usar los paquetes Dell Update Packages como parte de su estrategia de actualización del sistema.
- La *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.
- La *Guía del usuario de Dell Management Console* ofrece información para instalar, configurar y utilizar la consola. Dell Management Console es un software de administración de sistemas basada en web que permite descubrir e inventariar dispositivos en la red. También proporciona funciones avanzadas, como la supervisión de la condición y el rendimiento de los dispositivos conectados en red y capacidades de administración de parches para

los sistemas Dell.

- La *Guía del usuario de Dell Life Cycle 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. Unified Server Configurator también permite implementar un sistema operativo, configurar un arreglo redundante de discos independientes (RAID) y ejecutar diagnósticos para convalidar el sistema y el hardware conectado. Las funciones de servicios remotos permiten la detección automática de la plataforma del sistema a través de consolas de administración y optimizan las funciones de implementación remota de un sistema operativo. Estas funciones están disponibles a través de la interfaz de administración de hardware basada en servicios web que es proporcionada por el firmware de Lifecycle Controller.
- El *Glosario* de términos utilizados en este documento.

Obtención de asistencia técnica

Si en algún momento no entiende un procedimiento descrito en esta guía o si el producto no funciona como se espera, hay herramientas de ayuda a su disposición. Para obtener más información acerca de estas herramientas de ayuda, consulte "Obtención de ayuda" en el *Manual del propietario de hardware* del sistema.

Además, está disponible el servicio de capacitación y certificación Dell para empresas; para obtener más información, consulte **dell.com/training**. Es posible que este servicio no se ofrezca en todas las regiones.

Regresar a la página de contenido

Regresar a la página de contenido

Registros de Server Administrator

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Descripción general

Server Administrator le permite ver y administrar 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 comando. Los usuarios deben iniciar sesión con privilegios de Administrador para poder borrar registros, o con privilegios de Administrador o de Usuario avanzado para poder enviar registros por correo electrónico al contacto de servicio designado.

Para obtener información acerca de cómo ver los registros y crear informes a partir de la línea de comandos, consulte la *Guía del usuario de la interfaz de línea de comandos de Dell OpenManage Server Administrator*.

Al ver los registros de Server Administrator, puede hacer clic en **Ayuda** en la barra de navegación global para obtener información más detallada acerca de la ventana específica que está viendo. La ayuda del registro de Server Administrator está disponible para todas las ventanas a las que puede acceder el usuario, de acuerdo con el nivel de sus privilegios y de los grupos de hardware y software específicos que Server Administrator descubre en un sistema administrado.

Funciones integradas

Al hacer clic en el encabezado de una columna, los datos se ordenarán con base en la columna o el orden en la columna se invertirá. Además, cada ventana de registro contiene varios botones de tareas que se pueden utilizar para administrar y ofrecer asistencia al sistema.

Botones de tareas de la ventana de registro

- Haga clic en **Imprimir** para imprimir una copia del registro en la impresora predeterminada.
- Haga clic en **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 directorio que desee especificar.
- Haga clic en **Correo electrónico** para crear un mensaje de correo electrónico que incluya el contenido del registro como un archivo adjunto.
- Haga clic en **Borrar registro** para borrar todos los sucesos del registro.
- Haga clic en **Guardar como** para guardar el contenido del registro en un archivo **.zip**.
- Haga clic en **Actualizar** para volver a cargar el contenido del registro en el área de datos de una ventana de acciones.

Consulte "Botones de tareas" para obtener información adicional sobre el uso de los 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

Utilice el registro de hardware para buscar problemas potenciales en los componentes de hardware del sistema. En los sistemas Dell PowerEdge *x8xx*, *x9xx y xx1x*, el indicador de estado de registro de hardware cambia al estado crítico () cuando el archivo de registro alcanza el 100% de su capacidad. Hay dos registros de hardware disponibles, en función del sistema: el Registro de Embedded System Management (ESM) y el Registro de sucesos del sistema (SEL). Tanto el registro ESM como el SEL son 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 dispone de un icono de indicador de estado situado junto a su nombre. Una marca de verificación verde () indica que un componente está en una condición satisfactoria (normal). Un triángulo amarillo con un signo de admiración dentro () indica que un componente está en una condición de advertencia (no crítica) y requiere atención rápida. Una X roja () indica que un componente está en una condición de falla (crítica) y requiere atención inmediata. Un espacio en blanco ( ) indica que la condición de un componente es desconocida.

Para acceder al registro de hardware, haga clic en **Sistema**, luego en la ficha **Registros** y por último 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 indicador de estado situado junto al nombre de registro en la página de inicio de Server Administrator cambia de estado normal ( ) a estado no crítico ( ) cuando el archivo de registro alcanza el 80% de su capacidad. Asegúrese de borrar el registro de hardware cuando éste alcance el 80% de su capacidad. Si se permite que el registro llegue al 100% de la capacidad, los sucesos más recientes se descartarán del 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.

Utilice el registro de alertas para supervisar diversos sucesos del sistema. Server Administrator genera sucesos en respuesta a cambios del estado de los sensores y otros parámetros supervisados. Cada suceso de cambio de estado registrado en el registro de alertas consiste en un identificador exclusivo, denominado identificador de suceso, para cada categoría de fuente de suceso específica, así como un mensaje de suceso que describe el suceso. La identificación del suceso y el mensaje describen de forma exclusiva la gravedad y la causa del suceso, y proporcionan otros datos relevantes, como la ubicación del suceso y el estado previo del componente supervisado.

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

La información que aparece en el registro de alertas incluye:

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

NOTA: El historial de registros podría necesitarse para efectos de solución de problemas y de diagnóstico en el futuro. Por lo tanto, se recomienda guardar los archivos de registros.

Consulte la *Guía de referencia de mensajes de Server Administrator* para obtener información detallada sobre los mensajes de alerta.

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 visualizar la información del registro.

Utilice el registro de comandos para supervisar todos los comandos emitidos por los usuarios de Server Administrator. El registro de comandos realiza un seguimiento de los inicios y cierres de sesión, de la inicialización y las acciones de apagado del Systems Management Software, y registra la última vez que se borró el registro. El tamaño del archivo de registro de comandos puede especificarse de acuerdo a las necesidades.

Para acceder al registro de comandos, haga clic en **Sistema**, haga clic en la ficha **Registros** y luego 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 sus valores correspondientes

NOTA: El historial de registros podría necesitarse para efectos de solución de problemas y de diagnóstico en el futuro. Por lo tanto, se recomienda guardar los archivos de registros.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de Remote Access Controller

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

NOTA: *El controlador de administración de la placa base (BMC)* es admitido en los sistemas Dell PowerEdge *x8xx* y *x9xx*, mientras que *Integrated Dell Remote Access Controller (iDRAC)* es admitido en los sistemas Dell *xx0x* y *xx1x*.

Descripción general

Este capítulo proporciona información sobre la ubicación y el uso de las funciones de acceso remoto de BMC/iDRAC y DRAC.

El controlador de administración de la placa base (BMC) de Dell/ Integrated Dell Remote Access Controller (iDRAC) supervisa el sistema en busca de sucesos críticos mediante la comunicación con diversos sensores en la placa base, y envía alertas y sucesos de registro cuando ciertos parámetros exceden los umbrales preconfigurados. BMC/iDRAC es compatible con la especificación estándar industrial de la Interfaz de administración de plataforma inteligente (IPMI), lo que le permite configurar, supervisar y recuperar sistemas de manera remota.

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 el controlador de administración de la placa base (BMC) o Integrated Dell Remote Access Controller (iDRAC) del sistema, el DRAC puede configurarse para enviar alertas de correo electrónico sobre advertencias o errores relacionados con niveles de voltaje, temperaturas y velocidad de los ventiladores. DRAC también registra datos de sucesos y la más reciente pantalla de bloqueo (disponible sólo en sistemas que ejecutan el sistema operativo Microsoft Windows) para ayudar a diagnosticar la causa probable de un bloqueo del sistema.

Remote Access Controller proporciona acceso remoto a un sistema inoperable, permitiéndole recuperarlo y hacerlo funcionar de la manera más rápida posible. Remote Access Controller también ofrece notificaciones de alerta cuando un sistema está apagado y permite reiniciar un sistema de forma remota. Además, Remote Access Controller registra la causa probable 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 del controlador usando un explorador compatible.

Al utilizar Remote Access Controller, puede hacer clic en **Ayuda** en la barra de navegación global para obtener información detallada sobre la ventana específica que se está visualizando. La ayuda de Remote Access Controller está disponible para todas las ventanas a las que pueda acceder el usuario según el nivel de privilegios y los grupos de software y hardware específicos que Server Administrator descubre en el Managed System.

NOTA: Consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* para obtener más información acerca del BMC.

NOTA: Consulte la *Guía del usuario de Dell Remote Access Controller 4* para obtener más información sobre cómo usar el DRAC 4, o la *Guía del usuario de Dell Remote Access Controller 5* para obtener más información sobre cómo usar el DRAC 5.

NOTA: Consulte la Guía del usuario de *Integrated Dell Remote Access Controller* para obtener información detallada sobre la configuración y el uso de iDRAC.

La Tabla 5-1 muestra los nombres de campo de la interfaz gráfica del usuario y el sistema al que se aplican, cuando Server Administrator está instalado en el sistema.

Tabla 5-1. Disponibilidad del sistema para los siguientes nombres de campo de la interfaz gráfica del usuario

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

Consulte la *Matriz de compatibilidad de software de los sistemas Dell* para obtener más información sobre la compatibilidad de los sistemas con dispositivos de acceso remoto.

Server Administrator permite el acceso remoto dentro de banda a registros de sucesos, al control de la alimentación y a la información de estado de los sensores, y proporciona la capacidad de configurar el BMC/iDRAC. Es posible administrar BMC/iDRAC y DRAC mediante la interfaz gráfica del usuario de Server Administrator al hacer clic en el objeto **Acceso remoto**, que es un subcomponente del grupo **Chasis del sistema principal/Sistema principal**. El usuario puede realizar las siguientes tareas:

- Ver información básica

- Configurar el dispositivo de acceso remoto en una conexión de LAN
- Configurar el dispositivo de acceso remoto en una conexión de comunicación en serie en la LAN
- Configurar el dispositivo de acceso remoto en una conexión de puerto serie
- Configurar propiedades adicionales del dispositivo de acceso remoto
- Configurar los usuarios en el dispositivo de acceso remoto
- Definir alertas de filtro para sucesos de plataforma

El usuario puede ver información relativa al BMC/iDRAC y al DRAC, de acuerdo con el hardware que proporciona las capacidades de acceso remoto del sistema.

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

Además, la herramienta 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 del BMC solamente se pueden ver en sistemas Dell PowerEdge *x8xx* y *x9xx*.

Visualización de la información básica

El sistema le permite ver información básica acerca de BMC/iDRAC, la dirección IPv4 y DRAC. También puede restablecer la configuración de Remote Access Controller a los valores predeterminados. Para hacer esto:

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

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

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

Dispositivo de acceso remoto

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

Dirección IPv4

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

Dirección IPv6

- Origen 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: Sólo 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

El sistema permite configurar el dispositivo de acceso remoto para comunicarse a través de una conexión LAN.

1. Haga clic en el objeto **Gabinete modular→ Módulo del sistema/servidor→ Chasis del sistema principal / Sistema principal→ Acceso remoto**.

2. Haga clic en la ficha **Configuración**.

3. Haga clic en **LAN**.

   Aparece la página **Configuración de la LAN**.

   NOTA: El tráfico de administración de BMC/iDRAC no funciona correctamente si la LAN en la placa base (LOM) está formando equipo con tarjetas complementarias de adaptador de red.

4. Configure los siguientes detalles de la configuración del NIC:

   - Activar el NIC (esta opción está disponible en sistemas Dell PowerEdge *x9xx* y cuando DRAC está instalado. Seleccione esta opción para la formación de equipos del NIC. En sistemas Dell PowerEdge *x9xx*, puede formar equipos con varios NIC para obtener mayor redundancia.)

   NOTA: DRAC contiene un NIC Ethernet 10BASE-T/100BASE-T integrado y es compatible con TCP/IP. Este NIC tiene la dirección predeterminada 192.168.20.1 y la puerta de enlace predeterminada 192.168.20.1.

   NOTA: Si DRAC está configurado con la misma dirección IP que otro NIC de la misma red, se producirá un conflicto de dirección IP. DRAC dejará de responder a los comandos de red hasta que se cambie su dirección IP. DRAC se debe restablecer incluso si se resuelve el conflicto de dirección IP cambiando la dirección IP en el otro NIC.

   NOTA: Si se cambia la dirección IP de DRAC, éste se restablecerá. Si SNMP sondea el DRAC antes de que éste se inicialice, se registra una advertencia de temperatura porque no se transmite la temperatura correcta hasta que no se inicializa el DRAC.

   - Selección de NIC

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

   - Activar IPMI en la LAN
   - Origen de dirección IP
   - 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 *x9xx*).

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
   - Identificación de VLAN
   - Prioridad

6. Configure las siguientes propiedades de IPv4:

   - Origen de dirección IP
   - Dirección IP
   - Máscara de subred
   - Dirección de puerta de enlace

7. Configure las siguientes propiedades de IPv6:

   - Origen de dirección IP
   - Dirección IP
   - Longitud del prefijo
   - Puerta de enlace predeterminada
   - Fuente de dirección DNS
   - Servidor DNS preferido
   - Servidor DNS alternativo

   NOTA: Sólo puede configurar la información detallada de las direcciones IPv4 e IPv6 si activa las propiedades de IPv4 e IPv6 en la sección **Configuración adicional**.

8. Haga clic en **Aplicar cambios**.

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

Puede configurar el BMC para comunicación en una conexión de puerto serie. Para hacer esto:

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

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

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

Puede configurar el BMC/iDRAC para una comunicación de conexión en serie en la LAN (SOL). Para hacer esto:

1. Haga clic en **Gabinete modular→ Módulo del sistema/servidor→ 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**.

   Aparece 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 configuraciones del 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

Puede configurar las propiedades de IPv4 e IPv6 por medio de la ficha **Configuración adicional**. Para hacer esto:

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

Configuración de usuarios del dispositivo de acceso remoto

Los usuarios del dispositivo de acceso remoto pueden configurarse mediante la página **Acceso remoto**. Para acceder a esta página:

1. Haga clic en el objeto **Gabinete modular→ Módulo del sistema/servidor→ 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 del BMC/iDRAC.
3. Haga clic en **Identificación de usuario** para configurar un usuario nuevo o existente del 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 de marcación **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 del nivel de privilegios del usuario de LAN.
   - Seleccione el nivel de privilegio máximo permitido de usuario de puerto serie.
   - En sistemas Dell PowerEdge *x9xx*, 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: Con el DRAC instalado, se pueden configurar seis entradas de usuario adicionales. Esto da como resultado un total de 16 usuarios. Las reglas de nombre de usuario y contraseña son las mismas para los usuarios del BMC/iDRAC y del RAC. Cuando DRAC/iDRAC6 está instalado, las 16 entradas de usuario se asignan al DRAC.

Definición de alertas de filtro para sucesos de plataforma

Puede usar el Server Administrator Instrumentation Service para configurar las funciones más importantes de BMC, como los parámetros de los filtros de suceso de plataformas (PEF) y los destinos de las alertas. Para hacer esto:

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

   La ventana **Sucesos de plataforma** le permite realizar acciones individuales en sucesos de plataforma específicos. Puede seleccionar los sucesos para los que desea realizar acciones de apagado y generar alertas para acciones seleccionadas. También puede enviar alertas a los destinos con las direcciones IP específicas que elija.

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

   NOTA: El valor **Activar los filtros de alertas del sucesos de plataforma** activa o desactiva la generación de alertas de PEF. Es independiente de los valores de alerta de sucesos de plataformas individuales.

   NOTA: Las funciones de **Advertencia de sonda de alimentación del sistema** y **Falla de sonda de alimentación del sistema** no se admiten en los sistemas Dell que no tienen compatibilidad con PMBus, a pesar de que Server Administrator permite configurarlas.

   NOTA: En los sistemas Dell PowerEdge 1900, no se admiten los filtros de sucesos de plataforma **Advertencia PS/VRM/D2D, Falla PS/VRM/D2D** y **Suministro de energía ausente**, aun 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 seleccionadas 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:

   - **Ninguna**
     No lleva a cabo ninguna acción cuando el sistema operativo se bloquea o deja de funcionar.
   - **Reiniciar el sistema**
     Apaga el sistema operativo y comienza el inicio del sistema, realizando revisiones al BIOS y volviendo a cargar el sistema operativo.
   - **Realizar ciclo de encendido del sistema**
     Apaga la alimentación eléctrica al sistema, hace una pausa, enciende la alimentación y reinicia el sistema. El ciclo de encendido es útil cuando desea reinicializar componentes del sistema, como las unidades de disco duro.
   - **Apagar el sistema**
     Apaga la alimentación eléctrica del sistema.
   - **Reducción de alimentación**
     Detiene la CPU.

   NOTA: La reducción de la alimentación no se admite en todos los sistemas.

   PRECAUCIÓN: Si selecciona una acción de apagado de eventos de plataforma que no sea Ninguna ni Reducción de alimentación, el sistema se cerrará de manera forzada cuando el evento especificado se presente. El firmware inicia esta acción de apagado, que se ejecuta sin cerrar primero el sistema operativo ni las aplicaciones que estén abiertas.

6. Seleccione la casilla de marcación **Generar alerta** para que se envíen las alertas.

   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 cambios**.
8. Haga clic en **Volver a la página de sucesos de plataforma** para volver a la ventana **Filtros del suceso de plataforma**.

Definición del destino de la alerta del suceso de plataforma

También puede utilizar la ventana **Filtros del suceso de plataforma** para seleccionar un destino al cual se enviará una alerta para un suceso de plataforma. De acuerdo con el número de destinos que aparecen, puede configurar una dirección IP separada para cada dirección de destino. Se envía una alerta de suceso de plataforma a cada dirección IP de destino que configure.

1. Haga clic en **Configurar destinos** en la ventana **Filtros del suceso de plataforma**.

   La ventana **Configurar destinos** muestra varios destinos.

2. Haga clic en el número del destino que desea configurar.

NOTA: El número de destinos que puede configurar en un sistema dado puede variar.

3. Seleccione la casilla **Activar destino**.
4. Haga clic en **Número de destino** para introducir una dirección IP individual para ese destino. Esta dirección IP es a la dirección a la que se envía la alerta de suceso de plataforma.
5. Introduzca un valor en el campo **Cadena de comunidad** para que actúe como una contraseña para autentificar los mensajes enviados entre una estación de administración y un Managed System. La cadena de comunidad (que también se denomina nombre de comunidad) se envía en todos los paquetes entre la estación de administración y un Managed System.
6. Haga clic en **Aplicar cambios**.
7. Haga clic en **Volver a la página de sucesos de plataforma** para volver a la ventana **Filtros del suceso de plataforma**.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración y administración

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Administración de seguridad

Dell OpenManage Server Administrator proporciona seguridad a través del control de acceso basado en funciones (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 RBAC administra la seguridad determinando las operaciones que pueden ejecutar personas con funciones concretas. A cada usuario se le asigna una o varias funciones y a cada función se le asigna uno o varios privilegios de usuario permitidos a los usuarios con esa función. Con RBAC, la administración de la seguridad se corresponde muy estrechamente con la estructura de una organización.

Privilegios de usuario

Server Administrator otorga distintos derechos de acceso dependiendo de los privilegios del grupo asignado al usuario. Los cuatro niveles de usuario son: Usuario, Usuario avanzado, Administrador y Administrador avanzado.

- Los *usuarios* pueden ver la mayor parte de la información.
- Los *usuarios avanzados* pueden establecer valores para los umbrales de advertencia y configurar las acciones de alerta que se deberán realizar cuando ocurra un suceso de advertencia o de falla.
- Los *administradores* pueden configurar y realizar acciones de apagado, configurar acciones de recuperación automática en caso de que el sistema operativo de un sistema no responda y borrar registros de hardware, de sucesos y de comandos. Los *administradores* también pueden configurar el sistema para enviar correos electrónicos.
- Los *administradores avanzados* pueden ver y administrar información.

Server Administrator otorga acceso de sólo 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*. Consulte la Tabla 2-1.

Tabla 2-1. Privilegios de usuario

Privilegios de usuario	Tipo de acceso	
	Ver	Administrar
Usuario	Sí	No
Usuario avanzado	Sí	Sí
Administrador	Sí	Sí
Administrador avanzado (sólo en Linux)	Sí	Sí

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

La Tabla 2-2 resume los usuarios que tienen privilegios para acceder y administrar los servicios de Server Administrator.

Tabla 2-2. Niveles de privilegios del usuario de Server Administrator

Servicio	Nivel requerido de privilegios del usuario	
	Ver	Administrar
Instrumentación	U, UA, A, AA	UA, A, AA

Acceso remoto	U, UA, A, AA	A, AA
Storage Management	U, UA, A, AA	A, AA

En la Tabla 2-3 se definen las abreviaturas de los niveles de privilegios del usuario utilizadas en la Tabla 2-2.

Tabla 2-3. Leyenda para los niveles de privilegios del usuario de Server Administrator

U	Usuario
UA	Usuario avanzado
A	Administrador
AA	Administrador avanzado

Autentificación

El esquema de autentificación de Server Administrator garantiza la asignación de los tipos de acceso correctos a los privilegios de usuario correctos. Además, al invocar la interfaz de línea de comandos (CLI), el esquema de autentificación de Server Administrator valida el contexto en el que se ejecuta el proceso actual. Este esquema de autentificación garantiza que todas las funciones de Server Administrator, tanto si se accede a ellas desde la página de inicio de **Server Administrator** como si se accede desde la CLI, se autentifiquen correctamente.

Autentificación en Microsoft Windows

Para los sistemas operativos Microsoft Windows admitidos, la autentificación de Server Administrator usa la autentificación integrada de Windows (antes denominada NTLM). Este sistema de autentificación permite incorporar la seguridad de Server Administrator a un esquema de seguridad global para la red.

Autentificación en Red Hat Enterprise Linux y SUSE Linux Enterprise Server

En los sistemas operativos Red Hat Enterprise Linux y SUSE Linux Enterprise Server admitidos, Server Administrator usa varios métodos de autentificación basados en la biblioteca de módulos de autentificación conectables (PAM). Los usuarios pueden iniciar sesión en Server Administrator de manera local o remota a través de distintos protocolos de administración de cuentas, por ejemplo: LDAP, NIS, Kerberos y Winbind.

VMware ESX Server 4.X

VMware ESX Server usa la estructura de los módulos de autentificación conectables (PAM) para la autentificación cuando los usuarios acceden al host de ESX Server. La configuración de PAM para los servicios VMware se ubica en /etc/pam.d/vmware-authd, donde se almacenan rutas de acceso a los módulos de autentificación.

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

NOTA: En sistemas que ejecutan el sistema operativo VMware ESX Server 4.1, para iniciar sesión en Server Administrator, todos los usuarios necesitan privilegios de Administrador. Para obtener información sobre la asignación de funciones, consulte la documentación de VMware.

VMware ESXi Server 4.X

ESXi Server autentifica a los usuarios que acceden a los hosts ESXi mediante el cliente de VI/vSphere o el kit de desarrollo de software (SDK). La instalación predeterminada de ESXi hace uso de una base de datos de contraseñas local para la autentificación. Las transacciones de autentificación de ESXi con Server Administrator son también interacciones directas con el proceso **vmware-hostd**. Para asegurarse de que la autentificación funcione de manera eficaz para su sitio, realice tareas básicas, como definir usuarios, grupos, permisos y funciones, o configurar atributos de usuario, añadir sus propios certificados y determinar si desea o no usar SSL.

NOTA: En sistemas que ejecutan el sistema operativo VMware ESXi Server 4.1, para iniciar sesión en Server Administrator todos los usuarios necesitan privilegios de Administrador. Para obtener información sobre la asignación de funciones, consulte la documentación de VMware.

Cifrado

Se accede a Server Administrator mediante una conexión HTTPS segura la cual usa la tecnología de capa de conexión segura (SSL) para garantizar y proteger la identidad del sistema que se está administrando. Los sistemas operativos Microsoft Windows, Red Hat Enterprise Linux y SUSE Linux Enterprise Server admitidos usan Java Secure Socket Extension (JSSE) para proteger las credenciales de usuario y otros datos importantes que se transmiten por la conexión de socket cuando un usuario accede a la página de inicio de **Server Administrator**.

Asignación de los privilegios de usuarios

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

PRECAUCIÓN: Para proteger el acceso a los componentes importantes del sistema, asigne una contraseña a cada cuenta de usuario que pueda acceder al software Dell OpenManage. Los usuarios que no tienen una contraseña asignada no pueden iniciar sesión en Dell OpenManage en un sistema que ejecuta Windows Server 2003 debido a restricciones del sistema operativo.

PRECAUCIÓN: Desactive las cuentas de invitados de los sistemas operativos Windows compatibles para proteger el acceso a los componentes importantes del sistema. Considere cambiar el nombre de las cuentas de modo que las secuencias de comandos remotas no puedan activar las cuentas con ese nombre.

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

NOTA: Agregue nuevos usuarios al sistema operativo si desea agregar usuarios al software OpenManage. No es necesario crear nuevos usuarios dentro del 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 luego en **Usuario**→ **nuevo**.
3. Escriba la información de nombre de usuario adecuada en el cuadro de diálogo y luego haga clic en **Siguiente**.
4. Haga clic en **Siguiente** y luego 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 luego 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 y de Usuario avanzado, realice los siguientes pasos.

NOTA: Para realizar estos 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 desde la línea de comandos:

   useradd -d <*directorio_de_inicio*> -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 oprima <Entrar>.
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 desde la línea de comandos:

   `useradd -d <directorio_de_inicio> -g root <nombre_de_usuario>`

   NOTA: Establezca `root` como el grupo principal.

2. Escriba `passwd <nombre_de_usuario>` y oprima `<Entrar>`.

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: Conéctese como `root` o un usuario equivalente para realizar estos procedimientos.

1. Abra el archivo **omarolemap** que se encuentra en **/opt/dell/srvadmin/etc/omarolemap**.

2. Agregue la línea siguiente al archivo:

   `<nombre_de_usuario>[Tab]<nombre_del_host>[Tab]<derechos_de_acceso>`

   Tabla 2-4 muestra las leyendas para agregar la definición de funciones al archivo *omarolemap*

Tabla 2-4. Leyendas para agregar la definición de funciones en OpenManage Server Administrator

<nombre_de_usuario>	<nombre_del_host>	<derechos_de_acceso>
Nombre de usuario	Nombre de host	Administrador
(+)Nombre de grupo	**Domain** (Dominio)	Usuario
Comodín (*)	Comodín (*)	Usuario
[Tab] = \t (carácter de tabulador)		

La Tabla 2-5 muestra los ejemplos para agregar la definición de funciones al archivo *omarolemap*.

Tabla 2-5. Ejemplos para agregar la definición de funciones en OpenManage Server Administrator

<nombre_de_usuario>	<nombre_del_host>	<derechos_de_acceso>
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 su consideración cuando trabaje con el archivo **omarolemap**:

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

root	*	Administrador
+root	*	Usuario avanzado
*	*	Usuario

- No cambie los permisos de archivo ni el formato del archivo **omarolemap**.
- Server Administrator utiliza el privilegio de usuario predeterminado del sistema operativo si un usuario es degradado en el 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 +.
- Si existen entradas duplicadas de nombres o grupos de usuarios con el mismo <*nombre_del_host*>, Server Administrator utilizará los privilegios predeterminados de usuario del sistema operativo.
- También puede utilizar el *espacio* como delimitador de columnas en lugar de [Tab].

Creación de usuarios de Server Administrator para VMware ESX 4.X y ESXi 4.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 luego en **Usuarios**.
3. Haga clic con el botón derecho del mouse en cualquier parte de la tabla Usuarios y luego en **Agregar** para abrir el cuadro de diálogo **Agregar nuevo usuario**.
4. Ingrese un nombre de inicio de sesión, un nombre de usuario, un número de ID de usuario (UID) y una contraseña. No es obligatorio especificar el nombre de usuario y el UID. Si no especifica el UID, vSphere Client le asignará el primer UID disponible.
5. Para permitir que un usuario acceda al host de ESX/ESXi a través de un shell de comandos, seleccione **Otorgar acceso de shell a este usuario**. Los usuarios que accedan al host sólo por medio de 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 compatibles de Windows

NOTA: Para realizar este procedimiento, debe estar conectado con privilegios de administrador.

1. Abra la ventana **Administración del equipo**.
2. En el árbol de consola, expanda **Usuarios y grupos locales** y haga clic en **Usuarios**.
3. Haga doble clic en **Invitado** o en la cuenta de usuario **IUSR_nombre_de_sistema** para ver las propiedades de esos usuarios, o bien haga clic con el botón derecho del mouse en **Invitado** o **IUSR_nombre_de_sistema** y seleccione la opción **Propiedades**.
4. Seleccione **Cuenta deshabilitada** y haga clic en **Aceptar**.

   Aparecerá un círculo rojo con una X sobre el nombre de usuario. 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 compatibles. La asistencia de SNMP podría estar o no instalada, dependiendo del sistema operativo y de cómo se instaló. En la mayoría de los casos, SNMP se instala como parte del sistema operativo. Es necesario contar con un estándar de protocolo de administración de sistemas, como SNMP, para poder instalar Server Administrator.

El agente SNMP se puede configurar para cambiar el nombre de comunidad, activar operaciones Set y enviar capturas a una estación de administración. Para configurar el agente SNMP de manera tal que interactúe correctamente con las aplicaciones de administración, como Dell OpenManage IT Assistant, realice los procedimientos descritos en las siguientes secciones.

NOTA: La configuración predeterminada del agente SNMP comúnmente incluye un nombre de comunidad SNMP, como **public**. Por razones de seguridad, cambie los nombres predeterminados de comunidad SNMP. Para obtener información acerca de cómo cambiar los nombres de comunidad SNMP, consulte la sección correspondiente a continuación.

NOTA: Las operaciones Set de SNMP se encuentran desactivadas de manera predeterminada en las versiones 5.2 y posteriores de Server Administrator. Server Administrator ofrece asistencia para activar o desactivar las operaciones Set de SNMP en Server Administrator. Puede usar la página **Configuración de SNMP de Server Administrator** desde **Preferencias** o desde la interfaz de línea de comandos (CLI) de Server Administrator para activar o desactivar las operaciones Set de SNMP en Server Administrator. Para obtener más información acerca de la interfaz CLI de Server Administrator, consulte la *Guía del usuario de la interfaz de línea de comandos de Dell OpenManage Server Administrator*.

NOTA: Para que IT Assistant obtenga información de administración de un sistema que ejecuta Server Administrator, el nombre de comunidad utilizado por IT Assistant debe coincidir con el nombre de comunidad del sistema que ejecuta Server Administrator. Para que IT Assistant modifique la información o realice acciones en un sistema que ejecuta Server Administrator, el nombre de comunidad utilizado por IT Assistant debe coincidir con el nombre de comunidad que permite operaciones Set en el sistema que ejecuta Server Administrator. Para que IT Assistant reciba capturas (notificaciones de suceso asincrónicas) desde un sistema que ejecuta Server Administrator, el sistema que lo ejecuta debe estar configurado para enviar 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 4.0 admitidos para MIB VMware Proxy"
- "Configuración del agente SNMP en sistemas que ejecutan sistemas operativos VMware ESXi 4.0 admitidos"

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

Server Administrator utiliza los servicios SNMP proporcionados por el agente SNMP de Windows. El agente SNMP se puede configurar para cambiar el nombre de comunidad, activar operaciones Set y enviar capturas a una estación de administración. Para configurar el agente SNMP de manera que interactúe correctamente con las aplicaciones de administración, como IT Assistant, realice los procedimientos que se describen en las secciones siguientes.

NOTA: Consulte la documentación del sistema operativo para obtener detalles adicionales acerca de la configuración de SNMP.

Activación del acceso a SNMP mediante host remotos

De manera predeterminada, Windows Server 2003 no acepta paquetes SNMP desde hosts remotos. En los sistemas que ejecutan Windows Server 2003, debe configurar el servicio SNMP para que acepte paquetes SNMP de host remotos si planea administrar el sistema utilizando aplicaciones de administración de SNMP desde host remotos.

Para activar un sistema que ejecuta el sistema operativo Windows Server 2003 y recibir paquetes SNMP desde un host remoto, realice los siguientes pasos:

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 luego haga clic en **Propiedades**.

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

Cambio del nombre de comunidad SNMP

La configuración de los nombres de comunidad SNMP determina qué equipos pueden administrar su sistema por medio de SNMP. Para que las aplicaciones de administración puedan recuperar la información de administración de Server Administrator, el nombre de comunidad SNMP utilizado por las aplicaciones de administración debe coincidir con un nombre de comunidad SNMP configurado en el sistema de 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 luego haga clic en **Propiedades**.

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

5. Haga clic en la ficha **Seguridad** para agregar o modificar un nombre de comunidad.

   a. Para agregar un nombre de comunidad, haga clic en **Agregar**, en la lista **Nombres de comunidad aceptados**.

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

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

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

   c. Para cambiar un nombre de comunidad, seleccione un nombre de comunidad en la lista **Nombres de comunidad aceptados** y haga clic en **Editar**.

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

   d. Haga todos los cambios necesarios al nombre de comunidad del equipo que puede administrar su sistema en el cuadro de texto **Nombre de comunidad** y luego haga clic en **Aceptar**.

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

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

Activación de operaciones Set de SNMP

Las operaciones Set de SNMP deben estar activadas en el sistema de Server Administrator para poder cambiar los atributos de Server Administrator usando IT Assistant.

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 luego 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 haga clic en **Propiedades.**

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

5. Haga clic en la ficha **Seguridad** para acceder a los derechos de acceso de una comunidad.
6. Seleccione un nombre de comunidad en la lista **Nombres de comunidad aceptados** y haga clic en **Editar**.

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

7. Establezca los **Derechos de comunidad** en **LECTURA Y ESCRITURA** o **LECTURA Y CREACIÓN** y haga clic en **Aceptar**.

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

8. 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 cambios en el estado de los sensores y otros parámetros supervisados. Debe configurar uno o varios destinos de capturas en el sistema de Server Administrator para enviar las 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 a la lista de servicios hasta encontrar **Servicio SNMP**; haga clic con el botón derecho del mouse en **Servicio SNMP** y luego en **Propiedades**.

   Aparece 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 captura.

   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 captura, seleccione el nombre de la comunidad en el cuadro desplegable **Nombre de comunidad** y haga clic en **Agregar** en el cuadro **Destinos de capturas**.

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

   Introduzca el destino de captura y haga clic en **Agregar**.

   Aparece 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 usa los servicios SNMP proporcionados por el agente SNMP ***net-snmp***. Puede configurar el agente SNMP para cambiar el nombre de comunidad, activar operaciones Set y enviar capturas a una estación de administración. Para configurar el agente SNMP para una adecuada interacción con las aplicaciones de administración como, por ejemplo, IT Assistant, realice los procedimientos descritos en las secciones siguientes.

NOTA: Consulte la documentación del sistema operativo para obtener detalles adicionales acerca de la configuración de SNMP.

Configuración del control de acceso para el agente SNMP

La rama de la base de información de administración (MIB) implementada por Server Administrator se identifica por la identificación de objeto (OID) 1.3.6.1.4.1.674. Las aplicaciones de administración deben tener acceso a esta rama del árbol de MIB para administrar sistemas que ejecutan Server Administrator.

Para los sistemas operativos Red Hat Enterprise Linux y VMware ESXi 4.0, la configuración predeterminada del agente SNMP proporciona acceso de sólo lectura para la comunidad *public* sólo para la rama *system* de MIB-II (identificada mediante la OID 1.3.6.1.2.1.1) del árbol MIB. Esta configuración no permite que las aplicaciones de administración recuperen o cambien Server Administrator ni otra información de administración de 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 predeterminada de SNMP durante la instalación, intentará modificar la configuración del agente SNMP para proporcionar acceso de sólo lectura a todo el árbol MIB para la comunidad *public*. Server Administrator modifica el archivo de configuración del agente SNMP **/etc/snmp/snmpd.conf** de dos maneras:

El primer cambio es la creación de una vista de todo el árbol de la MIB, agregando la siguiente línea, si no existe:

```
view all included .1
```

El segundo cambio es la modificación de la línea *access* predeterminada para proporcionar acceso de sólo lectura a todo el árbol de la MIB para la comunidad *public*. Server Administrator busca la siguiente línea:

```
access notConfigGroup "" any noauth exact systemview none none
```

Si Server Administrator encuentra la línea anterior, la modifica para que diga:

```
access notConfigGroup "" any noauth exact all none none
```

Estos cambios a la configuración predeterminada del agente SNMP proporcionan acceso de sólo lectura a todo el árbol de la MIB para la comunidad *public*.

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.

El SNMP de Server Administrator se comunica con el agente SNMP mediante el protocolo de multiplexión de SNMP (SMUX). Cuando el SNMP de Server Administrator se conecta con el agente SNMP, el SNMP envía un identificador de objeto al agente SNMP para identificarse como interlocutor de SMUX. Como este identificador de objeto se debe configurar con el agente SNMP, Server Administrator agrega la siguiente línea al archivo de configuración del agente SNMP, **/etc/snmp/snmpd.conf**, durante la instalación, si no existe:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Cambio del nombre de comunidad SNMP

La configuración de los nombres de comunidad SNMP determina qué equipos pueden administrar su sistema por medio de SNMP. El nombre de comunidad SNMP utilizado por las aplicaciones de administración debe coincidir con un nombre de comunidad SNMP configurado en el sistema de Server Administrator para que las aplicaciones de administración puedan recuperar la información de administración de Server Administrator.

Para cambiar el nombre de comunidad SNMP que se utiliza para recuperar información de administración desde un sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP **/etc/snmp/snmpd.conf** y realice los pasos siguientes:

1. Encuentre la siguiente línea:

```
com2sec publicsec default public
```

o bien:

```
com2sec notConfigUser default public
```

2. Edite esta línea, reemplazando `public` con el nuevo nombre de comunidad SNMP. Una vez editada, la nueva línea debe ser:

```
com2sec publicsec default nombre_de_comunidad
```

o bien:

```
com2sec notConfigUser default nombre_de_comunidad
```

3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo:

```
service snmpd restart
```

Activación de operaciones Set de SNMP

Las operaciones Set de SNMP deben estar activadas en el sistema que ejecuta Server Administrator para poder cambiar los atributos de Server Administrator mediante IT Assistant.

Para activar las operaciones Set de SNMP en el sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP, **/etc/snmp/snmpd.conf**, y realice los siguientes pasos:

1. Encuentre la siguiente línea:

```
access publicgroup "" any noauth exact all none none
```

o bien:

```
access notConfigGroup "" any noauth exact all none none
```

2. Edite esta línea, reemplazando el primer `none` con `all`. Una vez editada, la nueva línea debe ser:

```
access publicgroup "" any noauth exact all all none
```

o bien:

```
access notConfigGroup "" any noauth exact all all none
```

3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo:

```
service snmpd restart
```

Configuración del sistema para enviar capturas a una estación de administración

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

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

1. Agregue la línea siguiente al archivo:

```
trapsink dirección_IP_nombre_de_comunidad
```

donde *dirección IP* es la dirección IP de la estación de administración y *nombre_de_comunidad* es el nombre de comunidad SNMP

2. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo:

```
service snmpd restart
```

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

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

NOTA: Consulte la documentación del sistema operativo para obtener más detalles acerca de la configuración de SNMP.

Acciones de instalación de SNMP de Server Administrator

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

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

Activación del acceso a SNMP desde hosts remotos

En sistemas operativos SUSE Linux Enterprise Server, la configuración predeterminada del agente SNMP proporciona acceso de sólo lectura a todo el árbol de la MIB para la comunidad *public* desde el host local solamente. Esta configuración no permite que las aplicaciones de administración de SNMP, como IT Assistant, que se ejecutan en otros host, descubran y administren correctamente los sistemas de Server Administrator. Si Server Administrator detecta esta configuración durante la instalación, introduce un mensaje en el archivo de registro del sistema operativo, **/var/log/messages**, para indicar que el acceso de SNMP está restringido al host local. Debe configurar el agente SNMP para activar el acceso de SNMP desde hosts remotos si planea administrar el sistema utilizando aplicaciones de administración de SNMP desde hosts remotos.

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

Para activar el acceso de 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. Encuentre la siguiente línea:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edite o copie esta línea, sustituyendo 127.0.0.1 con la dirección IP del host remoto. Una vez editada, la nueva línea debe ser:

   ```
   rocommunity public IP_address
   ```

   NOTA: Puede activar el acceso de 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 de 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:

1. Encuentre la siguiente línea:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edite esta línea eliminando 127.0.0.1. Una vez editada, la nueva línea debe ser:

   ```
   rocommunity public
   ```

3. 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

La configuración del nombre de comunidad SNMP determina las estaciones de administración que pueden administrar el sistema a través de SNMP. El nombre de comunidad SNMP utilizado por las aplicaciones de administración debe coincidir con un nombre de comunidad SNMP configurado en el sistema de Server Administrator, para que las aplicaciones de administración puedan recuperar la información de administración de Server Administrator.

Para cambiar el nombre predeterminado de comunidad SNMP que se utiliza para recuperar información de administración desde un sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP **/etc/snmp/snmpd.conf** y realice los pasos siguientes:

1. Encuentre la siguiente línea:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edite esta línea reemplazando `public` con el nuevo nombre de comunidad SNMP. Una vez editada, la nueva línea debe ser:

   ```
   rocommunity community_name 127.0.0.1
   ```

3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo:

   ```
   /etc/init.d/snmpd restart
   ```

Activación de operaciones Set de SNMP

Las operaciones Set de SNMP deben estar activadas en el sistema que ejecuta Server Administrator para poder cambiar los atributos de Server Administrator mediante IT Assistant. Para permitir el apagado remoto de un sistema desde IT Assistant, las operaciones Set de SNMP deben estar activadas.

NOTA: Las operaciones Set de SNMP no se requieren para reiniciar el sistema y cambiar la funcionalidad de la administración.

Para activar las operaciones Set de SNMP en un sistema que ejecuta Server Administrator, edite el archivo de configuración del agente SNMP, **/etc/snmp/snmpd.conf**, y realice los siguientes pasos:

1. Encuentre la siguiente línea:

   ```
   rocommunity public 127.0.0.1
   ```

2. Edite esta línea reemplazando `rocommunity` con `rwcommunity`. Una vez editada, la nueva línea debe ser:

   ```
   rwcommunity public 127.0.0.1
   ```

3. Para activar los cambios en la configuración de SNMP, reinicie el agente SNMP, escribiendo:

   ```
   /etc/init.d/snmpd restart
   ```

Configuración del sistema para enviar capturas a una estación de administración

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

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

1. Agregue la línea siguiente al archivo:

   ```
   trapsink IP_address community_name
   ```

   donde `dirección_IP` es la dirección IP de la estación de administración y `nombre_de_comunidad` es el nombre de la comunidad SNMP

2. 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 4.0 admitidos para MIB VMware Proxy

El servidor ESX4.0 puede ser administrado a través de un único puerto predeterminado 161 por medio del protocolo SNMP. Para que esto sea posible, `snmpd` está configurado para utilizar el puerto predeterminado 161, y `vmwarehostd` está configurado para utilizar un puerto diferente (no usado), por ejemplo, 167. Cualquier solicitud de SNMP en la rama MIB de VMWare se desviará al ***vmware-hostd*** por medio de la función de proxy del daemon ***snmpd***.

El archivo de configuración SNMP de VMWare puede modificarse manualmente en el servidor ESX o ejecutando el comando ***vicfg-snmp*** de la interfaz línea de comandos remota (RCLI) de VMWare desde un sistema remoto (Windows o Linux). Las herramientas RCLI pueden descargarse del sitio web de VMware (**http://www.vmware.com/download/vi/drivers_tools.html**).

A continuación se enumeran los pasos necesarios para la configuración.

1. Edite el archivo de configuración de SNMP de VMWare (**/etc/vmware/snmp.xml**) manualmente o ejecute los siguientes comandos vicfg-snmp para modificar los valores de configuración de SNMP. Eso incluye el puerto de escucha de SNMP, la cadena de comunidad, la dirección IP o del puerto de destino de la captura y el nombre de comunidad de captura, y luego active el servicio SNMP de VMWare.

   a. `vicfg-snmp.pl --server <dir_IP_de_ESX> -- username root --password <contraseña> -c <nombre_de_comunidad> -p X –t <dirección_IP_de_DMC>@162/<nombre_de_comunidad >`

   Donde X representa un puerto no usado. Para encontrar un puerto no usado, consulte el archivo **/etc/services** para ver la asignación de puertos para los servicios de sistema definidos. Además, para asegurarse de que el puerto seleccionado no está siendo utilizado actualmente por ninguna aplicación o servicio, ejecute el siguiente comando en el servidor ESX: `netstat –a command`

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

   b. Para habilitar el servicio SNMP de VMWare, ejecute el siguiente comando:

```
vicfg-snmp.pl --server <dir_IP_de_ESX> --username root --password <contraseña>

-E
```

c. Si desea ver los valores de configuración, ejecute el siguiente comando:

```
vicfg-snmp.pl --server <dir_IP_de_ESX> --username root --password <contraseña>

-s
```

Después de la modificación, el archivo de configuración aparecerá de la siguiente manera:

```
<?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. Ingrese la siguiente línea al final de **/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: `<dirección_IP_del_destino> <nombre_de_comunidad>`

Se requiere la especificación de trapsink para enviar capturas definidas en los MIB patentados.

5. Reinicie el servicio mgmt-vmware mediante el siguiente comando:

```
service mgmt-vmware restart
```

6. Reinicie el servicio snmpd mediante el siguiente comando:

```
service snmpd start
```

NOTA: Si srvadmin está instalado y los servicios ya se iniciaron, reinicie los servicios ya 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 4.0 admitidos

Server Administrator admite capturas SNMP en VMware ESXi 4.X. Server Administrator no admite las operaciones Get y Set de SNMP en VMWare ESXi 4.x ya que la compatibilidad necesaria con SNMP no está disponible. La interfaz de línea de comandos (CLI) de VMware vSphere se usa para configurar un sistema que ejecuta VMware ESXi 4.X para enviar capturas SNMP a una estación de administración.

NOTA: Para obtener más información acerca de cómo usar la CLI de VMware vSphere, consulte el sitio de asistencia de VMware en vmware.com/support.

Configuración del sistema para enviar capturas a una estación de administración

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

Para configurar un sistema ESXi que ejecuta Server Administrator para que envíe capturas a una estación de administración, realice los siguientes pasos:

1. Instale la CLI de VMware vSphere.
2. Abra un indicador de comandos en el sistema donde está instalada la CLI de VMware vSphere.
3. Cambie al directorio en el que está instalada la CLI VMware vSphere. La ubicación predeterminada en Linux es **/usr/bin**. La ubicación predeterminada en Windows es **C:\Program Files\VMware\VMware vSphere CLI\bin**.
4. Ejecute el siguiente comando:

   `vicfg-snmp.pl --server <servidor> --username <nombre_de_usuario> --password <contraseña> -c <comunidad> -t <hostname>/<comunidad>`

   donde `<servidor>` es el nombre de host o dirección IP del sistema ESXi, `<nombre_de_usuario>` es un usuario en el sistema ESXi, `<contraseña>` es la contraseña del usuario ESXi, `<comunidad>` es el nombre de comunidad SNMP y `<nombre_del_host>` es el nombre de host o dirección IP de Management Station.

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 mediante servidor de seguridad mientras instala Red Hat Enterprise Linux/SUSE Linux, el puerto SNMP en todas las interfaces de red externas se cerrará de forma predeterminada. Para activar las aplicaciones de administración de SNMP, como IT Assistant, para descubrir y recuperar información de Server Administrator, el puerto SNMP debe estar abierto al menos en una interfaz de red externa. Si Server Administrator detecta que el puerto SNMP no está abierto en el servidor de seguridad para ninguna interfaz de red externa, Server Administrator mostrará un mensaje de advertencia y escribirá un mensaje en el registro del sistema.

Para abrir el puerto SNMP desactivando el servidor de seguridad, abra una interfaz de red externa completa en el servidor de seguridad o abra el puerto 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 SNMP en RHEL utilizando uno de los métodos descritos anteriormente, siga estos pasos:

1. En el indicador de comandos de Red Hat Enterprise Linux, escriba setup y oprima **<Entrar>** para iniciar la utilidad de configuración de modo de texto.

   NOTA: Este comando está disponible sólo si ha realizado una instalación predeterminada del sistema operativo.

   Aparece el menú **Elegir una herramienta**.

2. Seleccione **Configuración del servidor de seguridad** utilizando la flecha hacia abajo y oprima **<Entrar>**.

   Aparece la pantalla **Configuración del servidor de seguridad**.

3. Oprima **<Tab>** para seleccionar **Nivel de seguridad**, y luego presione la barra espaciadora para seleccionar el nivel de seguridad que desea establecer. El nivel se seguridad seleccionado se indica con un asterisco.

   NOTA: Oprima <F1> para obtener más información acerca de los niveles de seguridad del servidor de seguridad. El número de puerto SNMP predeterminado es **161**. Si está utilizando la interfaz gráfica X Window del sistema, es posible que al presionar <F1> no obtenga información acerca de 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 a paso 7.

   b. Para abrir una interfaz de red completa o el puerto SNMP, seleccione **Alto, Medio** o **Activado** y continúe con paso 4.

d. Oprima **<Tab>** para ir a **Personalizar** y presione **<Entrar>**.

   Aparece la pantalla **Configuración del servidor de seguridad: Personalizar**.

5. Seleccione si desea abrir una interfaz de red completa o sólo el puerto SNMP en todas las interfaces de red.

   a. Para abrir una interfaz de red completa, oprima **<Tab>** para seleccionar uno de los dispositivos de confianza y luego presione la barra espaciadora. Un asterisco en la casilla a la izquierda del nombre del dispositivo indica que se abre la interfaz completa.

   b. Para abrir el puerto SNMP en todas las interfaces de red, oprima **<Tab>** para ir a **Otros puertos** y escriba `snmp:udp`.

6. Oprima **<Tab>** para seleccionar **Aceptar** y luego presione **<Entrar>**.

Aparece la pantalla **Configuración del servidor de seguridad**.

7. Oprima **<Tab>** para seleccionar **Aceptar** y luego presione **<Entrar>**.

   Aparece el menú **Elegir una herramienta**.

8. Oprima **<Tab>** para seleccionar **Salir** y presione **<Entrar>**.

Para abrir el puerto SNMP en SUSE Linux Enterprise Server, realice los siguientes pasos:

1. Configure SuSEfirewall2 mediante la ejecución del siguiente comando en una consola:
   ```
   a.# yast2 firewall
   ```

2. Utilice las teclas de flecha para acceder a **Servicios admitidos**.

3. Presione **Alt+d** para abrir el cuadro de diálogo **Puertos admitidos adicionales**.

4. Presione **Alt+T** para desplazar el cursor al cuadro de texto **Puertos TCP**.

5. Introduzca **snmp** en el cuadro de texto.

6. Presione **Alt-O** y `**Alt-N**' para avanzar a la siguiente pantalla.

7. Presione **Alt-A** para aceptar y aplicar los cambios.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de Server Administrator

Dell OpenManage Server Administrator
Versión 6.3 Guía del usuario

Inicio de la sesión de Server Administrator

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

Aparecerá la pantalla **Inicio de sesión** de **Server Administrator**. El puerto predeterminado de Dell OpenManage Server Administrator es 1311. Si es necesario, puede cambiar el puerto. Consulte "Servicio de conexión y configuración de seguridad de la administración de servidores de Dell Systems Management" para obtener instrucciones sobre la configuración de las preferencias del sistema.

Inicio y cierre de sesión

OpenManage Server Administrator ofrece tres tipos de inicio de sesión, a saber:

- Inicio de sesión en el sistema local de Server Administrator
- Inicio de sesión en Managed System de Server Administrator
- Inicio de sesión en Central Web Server

Inicio de sesión en el sistema local de Server Administrator

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

Utilice esta ventana de inicio de sesión para iniciar sesión en Server Administrator a través de un sistema local:

1. Escriba el **nombre de usuario** y **contraseña** en los campos correspondientes de la ventana **Inicio de sesión** de Systems Management.

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

2. Si el sistema ejecuta un sistema operativo Microsoft Windows y es miembro del dominio Windows, seleccione un dominio de la lista.

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

4. Haga clic en **Aceptar**.

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: Consulte la Guía del usuario de instalación y seguridad de OpenManage para obtener información sobre la configuración de Active Directory en sistemas sin CLI.

Inicio de sesión en Managed System de Server Administrator

Esta forma de inicio de sesión sólo se encuentra disponible si se instala el componente Web Server de Server Administrator. Para iniciar sesión en Server Administrator a fin de administrar un sistema remoto:

Método 1

1. Haga clic en el icono **Dell OpenManage Server Administrator** del escritorio.

2. Escriba la dirección IP del Managed System (sistema administrado), el nombre del sistema o el nombre de dominio completo (FQDN).

NOTA: Si introdujo el nombre del sistema o el FQDN, el host de Web Server de Dell OpenManage Server Administrator convierte el nombre del sistema o el FQDN en la dirección IP del Managed System. También puede introducir el número de puerto del Managed System. Por ejemplo, Nombre del host:Número de puerto o Dirección IP:Número de puerto.
Si se conectará a un nodo administrado de Citrix XenServer, use el puerto 5986 con el formato Nombre de host:Número de puerto o Dirección IP:Número de puerto.

3. Seleccione la casilla **Ignorar advertencias de certificado** si utiliza una conexión de Intranet.

4. Seleccione la **casilla Inicio de sesión de Active Directory**.Marque esta opción para iniciar sesión por medio del procedimiento de autentificación de Microsoft Active Directory. Deje la casilla en blanco si no utiliza el software Active Directory para controlar el acceso a la red. Consulte Uso del inicio de sesión de Active Directory.

5. Haga clic en **Aceptar**.

Método 2

Abra el explorador web, escriba una de las siguientes opciones en el campo de dirección y presione <Entrar>:

`https ://nombre de host:1311`

donde `nombre de host` es el nombre asignado para el sistema de nodo administrado y `1311` es el número de puerto predeterminado

o bien:

`https ://dirección IP:1311`

donde `dirección IP` es la dirección IP del Managed System y `1311` es el número de puerto predeterminado. Escriba `https ://` (y no `http://`) en el campo de dirección para recibir una respuesta válida del explorador.

NOTA: Debe tener derechos de usuario asignados previamente para poder iniciar sesión en Server Administrator. Para obtener instrucciones sobre la configuración de usuarios nuevos, consulte Configuración y administración.

Inicio de sesión en Central Web Server

Esta forma de inicio de sesión sólo se encuentra disponible si se instala el componente Web Server de Server Administrator. Utilice este método de inicio de sesión para administrar OpenManage Server Administrator Central Web Server:

1. Haga clic en el icono **Dell OpenManage Server Administrator** del escritorio. Aparecerá la página de inicio de sesión remoto.

   PRECAUCIÓN: La pantalla de inicio de sesión presenta una casilla que indica Ignorar advertencias de certificados. Utilice esta opción con prudencia. Se recomienda especialmente utilizarla sólo en entornos de Intranet confiables.

2. Haga clic en el vínculo **Administrar Web Server**, situado 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 **Aceptar**.

4. Seleccione la casilla **Inicio de sesión de Active Directory** para iniciar sesión por medio de Microsoft Active Directory. Consulte Uso del inicio de sesión de Active Directory.

5. Haga clic en **OK** (Aceptar).

Para terminar la sesión de Server Administrator, haga clic en **Cerrar sesión** en "Barra de navegación global". El botón **Cerrar sesión** se encuentra en la esquina superior derecha de cada página de inicio de **Server Administrator**.

NOTA: Al iniciar Server Administrator con Mozilla Firefox versión 3.0 y 3.5 o Microsoft Internet Explorer versión 7.0 ó 8.0, es posible que aparezca una página intermediaria de advertencia para informar que hay un problema con el certificado de seguridad. Para garantizar la seguridad del sistema, se recomienda enfáticamente que se genere un nuevo certificado X.509, que se vuelva a utilizar uno existente o que se importe un certificado raíz o una cadena de certificados desde una autoridad de certificación (CA). Para evitar encontrar tales mensajes de advertencia relacionados con el certificado, se deberá usar un certificado que provenga de una autoridad de certificados reconocida. Para obtener más información sobre la administración del certificado X.509, consulte "Administración de certificados X.509".

Para garantizar la seguridad del sistema, Dell recomienda enfáticamente importar un certificado raíz o una cadena de certificados de una autoridad de certificación (CA). Consulte la documentación de VMware para obtener información detallada.

NOTA: Si la autoridad de certificados del Managed System es válida y el Web Server de Server Administrator de todas formas indica un error de certificado no confiable, puede otorgar confiabilidad a la autoridad de certificados (CA) por medio del archivo **certutil.exe**. Consulte la documentación del sistema operativo para obtener información detallada sobre cómo acceder a este archivo **.exe**. En los sistemas operativos Windows admitidos, también puede utilizar el complemento de certificados como opción para importar certificados.

Uso del inicio de sesión de Active Directory

Seleccione la casilla **Inicio de sesión de Active Directory** para iniciar sesión por medio de la solución de esquema extendido de Dell en Active Directory.

Esta solución le permite proporcionar acceso a Server Administrator, con la capacidad de agregar/controlar usuarios y privilegios de Server Administrator para los usuarios ya existentes en el software Active Directory. Para obtener más información, consulte *Uso de Microsoft Active Directory* en la *Guía del usuario de instalación y seguridad de Dell OpenManage*.

inicio de sesión único

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

NOTA: Consulte el artículo de la base de conocimiento en **support.microsoft.com/default.aspx?scid=kb;en-us;Q258063** para obtener más información acerca del inicio de sesión único.

Para tener acceso a la máquina local, es necesario tener una cuenta en la máquina con los privilegios apropiados (Usuario, Usuario avanzado o Administrador). Los otros usuarios son autentificados con Microsoft Active Directory. Para ejecutar Server Administrator con autentificación de inicio de sesión único con Microsoft Active Directory, también se deben incluir los parámetros siguientes:

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

Donde *nombre del complemento* = *omsa*, *ita*, etc.

Por ejemplo:

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

Para ejecutar Server Administrator utilizando la autentificación de inicio de sesión único con las cuentas de usuario del sistema local, se debe llevar a cabo mediante los siguientes parámetros:

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

Donde *nombre del complemento* = *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 IT Assistant) 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 admitido

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

Los valores de seguridad de su explorador podrían evitar la ejecución de secuencias de comandos del lado del cliente que son usadas por Server Administrator. Para activar el uso de secuencias de comandos del lado del cliente, siga estos pasos en el sistema de administración remota.

NOTA: Si no ha configurado su explorador para activar el uso de secuencias de comandos del lado del cliente, puede recibir una pantalla en blanco al iniciar sesión en Server Administrator. En este caso, aparecerá un mensaje de error para indicarle que debe configurar los valores de su explorador.

Internet Explorer

1. En el explorador web, haga clic en **Herramientas**→ **Opciones de Internet**→ **Seguridad**.
2. Haga clic en el icono **Sitios de confianza**.
3. Haga clic en **Sitios**.
4. Copie la dirección web usada para acceder al Managed System remotamente desde la barra de dirección del explorador y péguela en el campo **Agregar este sitio web a la zona**.
5. Haga clic en **Nivel personalizado**.

   Para Windows Server 2003:

   - En **Varios**, seleccione el botón de radio **Permitir META ACTUALIZAR**.
   - En **Active Scripting**, seleccione el botón de radio **Activar**.
   - En **Active Scripting**, seleccione el botón de radio **Permitir la secuencia de comandos de los controles del explorador de web Internet Explorer**.

6. Haga clic en **Aceptar** para guardar la nueva configuración. Cierre el explorador e inicie sesión en Server Administrator.

Para permitir el inicio de sesión único en Server Administrator sin que se soliciten las credenciales del usuario, siga estos pasos:

1. En el explorador web, haga clic en **Herramientas**→ **Opciones de Internet**→ **Seguridad**.
2. Haga clic en el icono **Sitios de confianza**.
3. Haga clic en **Sitios**.
4. Copie la dirección web usada para acceder al Managed System remotamente desde la barra de dirección del explorador y péguela en el campo **Agregar este sitio web a la zona**.
5. Haga clic en **Nivel personalizado**.
6. En **Autentificación del usuario**, seleccione el botón de radio **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.
7. Haga clic en **Aceptar** para guardar la nueva configuración. Cierre el explorador e inicie sesión en Server Administrator.

Mozilla Firefox

1. Inicie el explorador.
2. Haga clic en **Editar**→ **Preferencias**.
3. Haga clic en **Avanzadas**→ **Scripts y plugins.**
4. Asegúrese de que la casilla **Navigator** esté seleccionada en **Activar JavaScript para**.
5. Haga clic en **Aceptar** para guardar la nueva configuración.
6. Cierre el explorador.
7. Inicie sesión en Server Administrator.

Página de inicio de Server Administrator

NOTA: No utilice los botones de su explorador web (como **Atrás** y **Actualizar)** cuando use Server Administrator. Utilice únicamente las herramientas de navegación de Server Administrator.

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

- Barra de navegación global: contiene vínculos que llevan a los servicios generales.
- Árbol del sistema: muestra todos los objetos del sistema visibles según los privilegios de acceso del usuario.
- Ventana de acciones: muestra las acciones de administración disponibles para el objeto del árbol del sistema seleccionado, dependiendo de los privilegios de acceso del usuario. En esta ventana se incluyen tres áreas funcionales:
  - Las fichas de acciones muestran las acciones o categorías de acciones principales disponibles para el objeto seleccionado, dependiendo de los privilegios de acceso del usuario.
  - Las fichas de acciones se dividen en subcategorías de todas las opciones secundarias disponibles para las fichas de acciones, dependiendo de los privilegios de acceso del usuario.
  - Área de datos: muestra información para el objeto del árbol del sistema, la ficha de acciones y la subcategoría seleccionadas, dependiendo de 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.

Tabla 3-1: muestra los nombres de campo de la interfaz gráfica del usuario y el sistema al que se aplican, cuando Server Administrator está instalado en el sistema.

Tabla 3-1. Disponibilidad del sistema para los siguientes nombres de campo de la interfaz gráfica del usuario

Nombre de campo de la interfaz gráfica del usuario	Sistema al que se aplica
Gabinete modular	Sistema modular
Módulo de servidor	Sistema modular
Sistema principal	Sistema modular

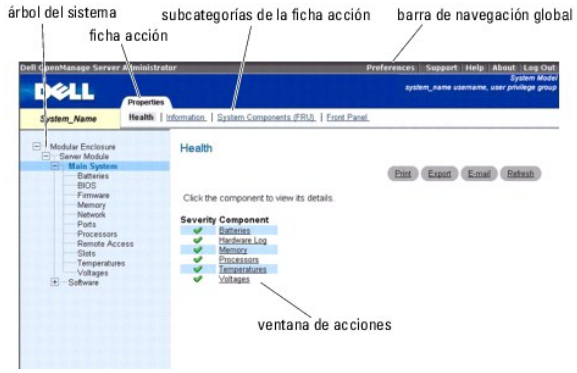
Sistema	Sistema no modular
Chasis del sistema principal	Sistema no modular

La Figura 3-1 muestra un ejemplo de la página de inicio de Server Administrator para un usuario conectado con privilegios de administrador en un sistema no modular.

Figura 3-1. Ejemplo de la página de inicio de Server Administrator: sistema no modular

La Figura 3-2 muestra un ejemplo de la página de inicio de Server Administrator para un usuario conectado con privilegios de administrador en un sistema modular.

Figura 3-2. 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 para ese objeto. Se puede desplazar por la ventana de acciones haciendo clic en las fichas de acciones para seleccionar categorías principales y haciendo clic en las subcategorías de las fichas de acciones para acceder a información más detallada o acciones más específicas. La información que se muestra en el área de datos de la ventana de acciones puede abarcar desde registros del sistema a indicadores de estado o medidas de sondas del sistema. Los elementos subrayados del área de datos de la ventana de acciones indican que existe 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 mayor nivel de detalle. Por ejemplo, al hacer clic en **Chasis del sistema principal/Sistema principal** bajo la subcategoría **Condición** de la ficha de acciones **Propiedades**, se muestra la condición de todos los componentes incluidos en el objeto Chasis del sistema principal/Sistema principal cuya condición se está supervisando.

NOTA: Los privilegios de usuario avanzado o administrador son necesarios para ver la mayoría de los objetos de árbol del sistema, componentes del sistema, fichas de acción y características de área de datos que se pueden configurar. Además, sólo los usuarios conectados con privilegios de administrador pueden acceder a las funciones críticas del sistema, como es la función de apagado que se incluye en la ficha **Apagado**.

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

La Tabla 3-2 muestra la disponibilidad de funciones de Server Administrator en sistemas modulares y no modulares. Una marca indica disponibilidad, en tanto una cruz indica la falta de disponibilidad de una función o característica.

Tabla 3-2. 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	✗	✓

		(a partir de sistemas *xx0x*)
Intromisión	✗	✓
Memoria	✓	✓
Red	✓	✓
Puertos	✓	✓
Administración de la alimentación	✓	✓ **(a partir de sistemas *xx0x*)**
Procesadores	✓	✓
Acceso remoto	✓	✓
Unidades flash extraíbles	✓	✓
Ranuras	✓	✓
Temperaturas	✓	✓
Voltajes	✓	✓
Gabinete modular (información del chasis y de CMC)	✓	✗

Barra de navegación global

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

- Al hacer clic en **Preferencias** se abre la página de inicio **Preferencias**. Consulte "Uso de la página de inicio de Preferencias".
- Al hacer clic en **Asistencia**, se establece conexión con el sitio web de asistencia técnica de Dell.
- Al hacer clic en **Ayuda**, se abre la ventana de ayuda contextual en línea. Consulte "Uso de la ayuda en línea".
- Al hacer clic en **Acerca de**, aparece la información de derechos de autor y la versión de Server Administrator.
- Al hacer clic en **Desconectar**, se finaliza la sesión actual del programa Server Administrator.

Árbol del sistema

El árbol del sistema aparece en el lado izquierdo de la página de inicio de Server Administrator y enumera los componentes del sistema que son visibles. Los componentes del sistema se clasifican según el tipo del componente. Al expandir el objeto principal denominado **Gabinete modular→ Módulo de sistema/servidor**, pueden aparecer las siguientes categorías principales de componentes del módulo del sistema/servidor: **Chasis del sistema principal/Sistema principal**, **Software** y **Almacenamiento**.

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

Ventana de acciones

Al hacer clic en un elemento del árbol del sistema, aparecen detalles acerca del componente u objeto en el área de datos de la ventana de acciones. Al hacer clic en una ficha de acciones, aparecen todas las opciones disponibles del usuario como una lista de subcategorías.

Al hacer clic en un objeto del árbol del módulo del sistema o servidor, se abre la ventana de acciones del componente, en la que aparecen las fichas de acciones disponibles. El área de datos presenta de manera predeterminada una subcategoría preseleccionada de la primera ficha de acciones para el objeto seleccionado. Esta subcategoría preseleccionada suele ser la primera opción. Por ejemplo, al hacer clic en el objeto **Chasis del sistema principal/Sistema principal**, se abre una ventana de acciones en cuya área de datos aparecen la ficha de acción **Propiedades** y la subcategoría **Condición**.

Área de datos

El área de datos se encuentra bajo las fichas de acciones en el lado derecho de la página de inicio. En el área de datos se realizan las tareas o se ven detalles acerca de los componentes del sistema. El contenido de la ventana depende del objeto del árbol del sistema y de la ficha de acciones seleccionados. Por ejemplo, al seleccionar **BIOS** en el árbol del sistema, se selecciona la ficha **Propiedades** de manera predeterminada y en el área de datos aparece la información de versión del BIOS del sistema. El área de datos de la ventana de acciones contiene numerosas características comunes, incluyendo indicadores de estado, botones para tareas, elementos subrayados e 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 sistema o servidor

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 3-3. Indicadores de estado de los componentes del módulo del sistema o servidor

	Una marca de verificación verde indica que un componente está en buen estado (normal).
	Un triángulo amarillo que contiene un signo de exclamación indica que el componente tiene una condición de advertencia (no crítica). Una condición de advertencia se produce cuando una sonda u otra herramienta de supervisión detecta una lectura para un componente que se encuentra entre determinados valores mínimos y máximos. Una condición de advertencia requiere atención rápida.
	Una X roja indica que un componente tiene una condición de falla (crítica). Una condición crítica se produce cuando una sonda u otra herramienta de supervisión detecta una lectura para un componente que se encuentra entre determinados valores mínimos y máximos. Una condición crítica requiere atención inmediata.
	Un espacio en blanco indica que la condición del componente no se conoce.

Botones de tareas

La mayoría de las ventanas abiertas desde la página de inicio de Server Administrator contienen al menos cuatro botones de tareas: **Imprimir**, **Exportar**, **Correo electrónico** y **Actualizar**. Se incluyen otros botones de tareas en las ventanas específicas de Server Administrator. Por ejemplo, las ventanas de registro también contienen los botones de tareas **Guardar como** y **Borrar registro**. Para obtener información específica sobre los botones de tareas individuales, haga clic en **Ayuda** en cualquier página de inicio de Server Administrator para ver información detallada sobre la ventana específica que está visualizando.

- Al hacer clic en **Imprimir**, la impresora predeterminada imprime una copia de la ventana abierta.
- Al hacer clic en **Exportar** se genera un archivo de texto que contiene una lista de los valores para cada campo de datos de la ventana activa. El archivo de exportación se guardará en la ubicación que usted especifique. Consulte "Configuración de las preferencias del usuario y del sistema" para obtener instrucciones sobre cómo personalizar el delimitador que separa los valores de los campos de datos.
- Al hacer clic en **Correo electrónico**, se crea un mensaje de correo electrónico dirigido al destinatario designado. Consulte "Configuración de las preferencias del usuario y del sistema" para obtener instrucciones de configuración del servidor de correo electrónico y el destinatario predeterminado de correo electrónico.
- 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.

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

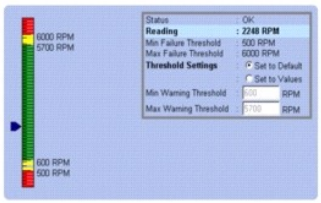
Elementos subrayados

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

Las sondas de temperatura, de ventiladores y de voltaje están representadas por un indicador de medida. Por ejemplo, Figura 3-3 muestra lecturas de una sonda de ventilador de la CPU del sistema.

Figura 3-3. Indicador de medida



Uso de la ayuda en línea

La ayuda contextual en línea está disponible para cada ventana de la página de inicio de Server Administrator. Al hacer clic en **Ayuda** en la barra de navegación global, se abre una ventana de ayuda independiente que contiene información detallada sobre la ventana específica que se está viendo. La ayuda en línea está diseñada para guiarle por las acciones específicas necesarias para llevar a cabo todos los aspectos de los servicios del Server Administrator. La ayuda en línea está disponible para todas las ventanas que se pueden ver, organizada de acuerdo con los grupos de software y hardware que Server Administrator descubre en el sistema y con el nivel de privilegios 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 siguientes son las opciones de configuración de la página de inicio Preferencias que se encuentran disponibles:

- Configuración general
- Server Administrator

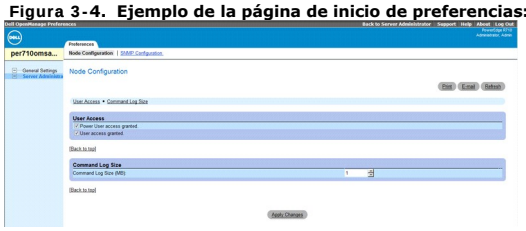
Podrá ver la ficha **Preferencias** después de iniciar sesión para administrar un sistema remoto. Esta ficha también se encuentra disponible al iniciar sesión para administrar el servidor web (Web Server) de Server Administrator o el sistema local.

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

- La barra de navegación global proporciona vínculos a servicios generales.
  - Al hacer clic en **Regresar a Server Administrator**, se regresa a la página de inicio de Server Administrator.
- 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 las categorías de preferencias para el Managed System o el Web Server de Server Administrator.
- La ventana de acciones muestra los valores y las preferencias disponibles para el Managed System o el Web Server de Server Administrator.

La Figura 3-4 muestra un ejemplo de la distribución de la página de inicio de preferencias.

Figura 3-4. Ejemplo de la página de inicio de preferencias: Managed System



Preferencias en el Managed System

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 los usuarios con privilegios de Usuario o de Usuario avanzado. De acuerdo con los privilegios del grupo de usuarios, la ventana de acciones del objeto Server Administrator puede incluir la ficha **Preferencias**.

En la ficha Preferencias, usted puede:

- Activar o desactivar el acceso de usuarios con privilegios de usuario o de usuario avanzado.
- Configurar el tamaño del registro de comandos
- Configurar SNMP

Preferencias de Web Server de Server Administrator

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

Debido a la separación entre el Web Server de Server Administrator y el Managed System, las siguientes opciones aparecen cuando inicia sesión mediante el vínculo Administrar Web Server:

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

Para obtener más información sobre cómo acceder a estas funciones, consulte "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 establecen desde la página de inicio de **Preferencias**.

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

Siga estos pasos para configurar las preferencias del usuario:

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

   Aparece la página de inicio de **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 cambios**.

   NOTA: Al hacer clic en **Correo electrónico** en cualquier ventana, se envía un mensaje de correo electrónico con un archivo HTML adjunto de la ventana a la dirección de correo electrónico designada.

4. Para cambiar el aspecto de la página de inicio, seleccione otro valor en los campos **apariencia** o **esquema** y haga clic en **Aplicar cambios**.

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

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

   Aparece la página de inicio de **Preferencias**.

2. Haga clic en **Configuración general** y luego en la ficha **Web Server**.

3. En la ventana **Preferencias del servidor,** establezca las opciones conforme sea necesario.

   - La función **Tiempo de espera de la sesión** puede establecer un límite sobre la cantidad de tiempo que una sesión de Server Administrator puede permanecer activa. Seleccione el botón de radio **Activar** para permitir que finalice la sesión de Server Administrator si no hay ninguna interacción por parte del usuario durante un determinado número de minutos. Los usuarios cuyas sesiones excedan el tiempo de espera deberán conectarse de nuevo para continuar. Seleccione el botón de radio **Desactivar** para desactivar la función de tiempo de espera de sesión 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 a uno no válido o a un número de puerto en uso, se puede impedir que otras aplicaciones o exploradores accedan al Server Administrator en el Managed System. Consulte la *Guía del usuario de seguridad e instalación de Dell OpenManage* para ver la lista de puertos predeterminados.

   - El campo **Dirección IP a la cual enlazar** especifica las direcciones IP para el Managed System a las que se enlaza Server Administrator cuando inicia una sesión. Seleccione el botón de radio **Todas** para enlazar con todas las direcciones IP aplicables para el sistema. Seleccione el botón de radio **Específica** para enlazar con una dirección IP específica.

   NOTA: Si se cambia el valor de **Dirección IP a la cual enlazar** a otro valor que no sea **Todas**, es posible que otras aplicaciones o exploradores no puedan acceder a Server Administrator en el Managed System.

   - Los campos **Nombre de servidor SMTP** y **Sufijo DNS para servidor SMTP** especifican el protocolo de transferencia simple de correo (SMTP) y el sufijo del servidor de nombres de dominio (DNS) de la empresa u organización. Para que el Server Administrator pueda enviar mensajes de correo electrónico, debe teclear la dirección IP y el sufijo DNS del servidor SMTP de la empresa u organización en los campos correspondientes.

   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 sólo aparece al iniciar sesión para administrar Web Server de Server Administrator.

   - El campo **Vínculo de asistencia** especifica la dirección URL de la entidad empresarial que proporciona asistencia al Managed System.
   - El campo **Delimitador personalizado** especifica el carácter utilizado para separar los campos de datos en los archivos creados utilizando el botón **Exportar**. El carácter **;** es el delimitador predeterminado. Otras opciones son **!**, **@**, **#**, **$**, **%**, **^**, *****, **~**, **?**, **|** y **,**.
   - El campo **Cifrado SSL** especifica los niveles de cifrado de las sesiones HTTPS aseguradas. Los niveles de cifrado disponibles incluyen **Negociación automática** y **128 bits o superior**.
     - **Negociar automáticamente**: Para permitir la conexión por medio de un explorador con cualquier nivel de cifrado. El explorador negocia automáticamente con el Web Server de Server Administrator y usa el mayor nivel de cifrado que esté disponible para la sesión. Los exploradores heredados que tienen cifrados más débiles podrán conectarse a Server Administrator.
     - **128 bit o superior**: Para permitir conexiones provenientes de exploradores con niveles de cifrado de 128 bit o superior. Para las sesiones establecidas, se aplica alguno de los siguientes paquetes de cifrado, en función del explorador:

       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

- **Algoritmo de firma de clave** muestra los algoritmos de firma admitidos. Seleccione un algoritmo de la lista desplegable. Si selecciona SHA 512 o SHA 256, asegúrese de que su sistema operativo y su navegador sean compatibles con este algoritmo. Si selecciona una de estas opciones, y no es compatible con su sistema operativo o navegador, Server Administrator mostrará el mensaje de error `cannot display the webpage (no se puede mostrar la página)`. Este campo es exclusivo para los certificados autofirmados y autogenerados de Server Administrator. La lista desplegable aparecerá en gris si se importan o generan certificados nuevos en Server Administrator

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

NOTA: Reinicie el Web Server de Server Administrator para que los cambios surtan efecto.

NOTA: Si el nivel de cifrado está establecido como **128 bits o superior**, podrá acceder o modificar la configuración de Server Administrator a través de un explorador que tenga niveles de cifrado iguales o mayores.

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

Administración de certificados X.509

Los certificados web son necesarios para garantizar la identidad de un sistema remoto y para asegurar que la información intercambiada con el mismo no pueda ser vista ni cambiada por otros usuarios. Para garantizar la seguridad del sistema, se recomienda enfáticamente lo siguiente:

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

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

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

Puede utilizar esta opción para realizar lo siguiente:

- **Generar un nuevo certificado X.509**: Use esta opción para crear un certificado de acceso a Server Administrator.
- **Mantenimiento de certificado**: Esta opción le permite seleccionar un certificado ya existente que pertenece a su empresa y usarlo para controlar el acceso a Server Administrator.
- **Importar un certificado raíz**: Esta opción le permite importar un certificado raíz, así como la respuesta al certificado (en formato PKCS#7) proveniente de la autoridad de certificados de confianza.
- **Importar una cadena de certificados de una CA**: Esta opción le permite importar la respuesta al certificado (en formato PKCS#7) de la autoridad de certificados de confianza. Verisign, Thawte y Entrust son algunas de las autoridades de certificados confiables.

Fichas de acciones de Web Server de Server Administrator

Al iniciar sesión para administrar Web Server de Server Administrator aparecerán las siguientes fichas de acciones:

- Apagado
- Registros
- Administración de sesiones

Administración de Server Administrator

Server Administrator se inicia automáticamente cada vez que se reinicia el Managed System. Para iniciar, detener o reiniciar automáticamente el Server Administrator, utilice las siguientes instrucciones.

NOTA: Para administrar Server Administrator, debe iniciar sesión con privilegios de administrador (en el caso de sistemas operativos admitidos Citrix XenServer, Red Hat Enterprise Linux o SUSE Linux Enterprise Server, debe iniciar sesión como `root`).

Inicio de Server Administrator

Sistemas operativos Microsoft Windows admitidos

Para iniciar Server Administrator en los sistemas que ejecutan un sistema operativo Windows admitido, realice los siguientes pasos:

1. Abra la ventana **Servicios**.
2. Haga clic con el botón derecho del mouse en el icono del **Servicio de conexión de la administración de servidores Dell Systems Management (DSM SA)**.
3. Haga clic en **Inicio**.

Sistemas operativos admitidos Citrix XenServer, Red Hat Enterprise Linux y SUSE Linux Enterprise Server

Para iniciar Server Administrator en sistemas que ejecutan un sistema operativo admitido Citrix XenServer, Red Hat Enterprise Linux o SUSE Linux Enterprise Server, ejecute el siguiente comando desde la línea de comandos:

```
dsm_om_connsvc start
```

Detención de Server Administrator

Sistemas operativos Microsoft Windows admitidos

Para detener Server Administrator, siga estos pasos:

1. Abra la ventana **Servicios**.
2. Haga clic con el botón derecho del mouse en el icono **Servicio de conexión SA de DSM**.
3. Haga clic en **Detener**.

Sistemas operativos admitidos Citrix XenServer, Red Hat Enterprise Linux y SUSE Linux Enterprise Server

Para detener Server Administrator en sistemas que ejecutan un sistema operativo admitido Citrix XenServer, Red Hat Enterprise Linux o SUSE Linux Enterprise Server, ejecute el siguiente comando desde la línea de comandos:

```
dsm_om_connsvc stop
```

Reinicio de Server Administrator

Sistemas operativos Microsoft Windows admitidos

Para reiniciar Server Administrator, siga estos pasos:

1. Abra la ventana **Servicios**.
2. Haga clic con el botón derecho del mouse en el icono **Servicio de conexión SA de DSM**.
3. Haga clic en **Reiniciar**.

Sistemas operativos admitidos Citrix XenServer, Red Hat Enterprise Linux y SUSE Linux Enterprise Server

Para reiniciar Server Administrator en sistemas que ejecutan un sistema operativo admitido Citrix XenServer, Red Hat Enterprise Linux o SUSE Linux Enterprise Server, ejecute el siguiente comando desde la línea de comandos:

```
dsm_om_connsvc restart
```

Uso de la interfaz de línea de comando de Server Administrator

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

En muchos casos, la CLI permite a un usuario que desea realizar una tarea muy específica recuperar información sobre el sistema rápidamente. Por ejemplo, mediante el uso de comandos de CLI los administradores pueden escribir secuencias de comandos o programas por lotes para ejecutarlos en determinados momentos. Al ejecutar estos programas, pueden capturar informes sobre componentes de interés, como las rpm del ventilador. Con secuencias de comandos adicionales, la CLI puede emplearse para capturar datos durante periodos de elevado uso del sistema y compararlos con las mismas medidas en períodos de

poco uso. Los resultados de los comandos se pueden enviar a un archivo para analizarlos más tarde. Estos informes pueden ayudar a los administradores a obtener información que se puede utilizar para ajustar patrones de uso, justificar compras de nuevos recursos del sistema o concentrarse en el estado de un componente con problemas.

Para obtener instrucciones completas sobre la funcionalidad y el uso de la CLI, consulte la *Guía del usuario de la interfaz de línea de comando de Dell OpenManage Server Administrator*.

Regresar a la página de contenido