Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Notas y precauciones

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

PRECAUCIÓN: Un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos si no se siguen las instrucciones.

Junio de 2009

Regresar a la página de contenido

Glosario

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Active Directory

Active Directory es un sistema centralizado y estandarizado que automatiza la administración de red de los datos de usuario, la seguridad y los recursos distribuidos y hace posible las operaciones con otros directorios. Active Directory está diseñado especialmente para los entornos de red distribuidos.

ARP

Sigla de Address Resolution Protocol (protocolo para resolución de direcciones), que es un método para encontrar la dirección Ethernet de un host a partir de su dirección de Internet.

ASCII

Sigla de American Standard Code for Information Interchange (código estándar estadounidense para intercambio de información), que es una representación de códigos que se usa para mostrar o imprimir letras, números y otros caracteres.

BIOS

Sigla de Basic Input/Output System (sistema básico de entradas y salidas), que es la parte del software de sistema que proporciona la interfaz al nivel más bajo a los dispositivos periféricos y que controla la primera fase del proceso de inicio del sistema, incluida la instalación del sistema operativo en la memoria.

bus

Conjunto de conductores que conectan las distintas unidades funcionales en un equipo. Los buses reciben su nombre en función del tipo de datos que llevan, por ejemplo, bus de datos, bus de direcciones o bus PCI.

CA

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis fiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Una vez que la autoridad de certificados recibe la CSR, revisan y verifican la información contenida en ella. Si el candidato cumple los estándares de seguridad de la autoridad de certificados, ésta emite un certificado al candidato que lo identifica de forma exclusiva para transacciones a través de redes y en Internet.

CD

Abreviatura de compact disc (disco compacto).

CHAP

Sigla de Challenge-Handshake Authentication Protocol (protocolo de autenticación de establecimiento de conexión por desafío), que un esquema de autenticación utilizado por los servidores PPP para validar la identidad del iniciador de la conexión.

CIM

Sigla de Common Information Model (modelo de información común), que es un protocolo diseñado para la administración de sistemas en una red.

CLI

Abreviatura de Command-Line Interface (interfaz de línea de comandos).

CLP

Abreviatura de Command-Line Protocol (protocolo de línea de comandos).

CSR

Abreviatura de Certificate Signing Request (solicitud de firma de certificado).

DHCP

Abreviatura de Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host), que es un protocolo que proporciona los medios para distribuir direcciones IP de manera dinámica a los equipos en una red de área local.

DLL

Abreviatura de Dynamic Link Library (biblioteca de vínculo dinámico), que es una biblioteca de pequeños programas, a los que un programa más grande que se ejecuta en el sistema puede llamar cuando sea necesario. El programa pequeño que permite al programa más grande comunicarse con un dispositivo específico, como una impresora o un escáner, a menudo se empaqueta como un programa (o archivo) DLL.

DDNS

Abreviatura de Dynamic Domain Name System (sistema de nombres de dominio dinámicos).

Dirección MAC

Sigla de dirección Media Access Control (control de acceso a medios), que es una dirección única incorporada en los componentes físicos de una tarjeta de interfaz de red.

disco RAM

Programa residente en la memoria que emula una unidad de disco duro. El iDRAC6 mantiene un disco RAM en su memoria.

DMTF

Abreviatura de Distributed Management Task Force (equipo de trabajo de administración distribuida).

DNS

Abreviatura de Domain Name System (sistema de nombres de dominio).

DSU

Abreviatura de Disk Storage Unit (unidad de almacenamiento en disco).

esquema ampliado

Solución que se usa con Active Directory para determinar el acceso de los usuarios al iDRAC6; utiliza objetos de Active Directory definidos por Dell.

esquema estándar

Solución que se usa con Active Directory para determinar el acceso de los usuarios al iDRAC6; utiliza únicamente objetos de grupo de Active Directory.

Estación de administración

La estación de administración es sistema desde el cual un administrador administra remotamente un sistema Dell que tiene un iDRAC6.

excepción SNMP

Notificación (evento) generada por el iDRAC6 que contiene información sobre los cambios de estado en el sistema administrado o sobre problemas potenciales de hardware.

FQDN

Sigla de Fully Qualified Domain Names (nombres de dominio completos). Microsoft® Active Directory® sólo admite nombres de dominio completos de 64 bytes o menos.

FSMO

Siglas de Flexible Single Master Operation (operación maestra única y flexible). Es la manera en la que Microsoft garantiza la atomicidad de la operación de ampliación.

GMT

Abreviatura de Greenwich Mean Time (hora media de Greenwich), que es la hora estándar común a todos los lugares en el mundo. La GMT refleja nominalmente la hora solar media sobre el meridiano principal (longitud 0) que atraviesa el observatorio de Greenwich en las afueras de Londres, Reino Unido.

GPIO

Abreviatura de General Purpose Input/Output (entrada/salida de propósito general).

GRUB

Sigla de GRand Unified Bootloader, un cargador nuevo de Linux de uso común.

GUI

Abreviatura de Graphical User Interface (interfaz gráfica para el usuario), que se refiere a una interfaz en pantalla de equipos que usa elementos como ventanas, cuadros de diálogo y botones, contrario a una interfaz con petición de comandos, en la cual toda la interacción de los usuarios se muestra y se teclea en texto.

iAMT

Tecnología de administración activa de Intel®: proporciona capacidades de administración de sistemas más seguras sin importar si el equipo está encendido o apagado, o si el sistema operativo no responde.

ICMB

Abreviatura de Intelligent Enclosure Management Bus (bus de administración de carcasa inteligente).

ICMP

Abreviatura de Internet Control Message Protocol (protocolo de mensajes de control de Internet).

ID

Abreviatura para identificación, usada comúnmente al referirse a la identificación de un usuario (Id. del usuario) o identificación de un objeto (Id. del objeto).

iDRAC6

Sigla de Integrated Dell Remote Access Controller (controlador de acceso remoto integrado de Dell), el sistema de supervisión y control integrado en el chip de los servidores Dell 11G PowerEdge.

IP

Abreviatura de Internet Protocol (protocolo de Internet), que es la capa de red de TCP/IP. El IP proporciona encaminamiento, fragmentación y reensamblaje de paquetes.

IPMB

Abreviatura de Intelligent Platform Management Bus (bus de administración de plataforma inteligente), que es un bus que se utiliza en la tecnología de administración de sistemas.

IPMI

Abreviatura de Intelligent Platform Management Interface (interfaz de administración de plataformas inteligentes), que es una parte de la tecnología de administración de sistemas.

Kbps

Abreviatura de kilobits por segundo, que es una velocidad de transferencia de datos.

LAN

Abreviatura de Local Area Network (red de área local).

LDAP

Abreviatura de Lightweight Directory Access Protocol (protocolo ligero de acceso a directorios).

LED

Abreviatura de Light-Emitting Diode (diodo emisor de luz).

LOM

Abreviatura de Local area network On Motherboard (red de área local integrada a la placa base).

LUN

Sigla de Logical Unit (unidad lógica).

MAC

Sigla de Media Access Control (control de acceso a medios), que es una subcapa de red entre un nodo de red y la capa física de la red.

MAP

Abreviatura de Manageability Access Point (punto de acceso de administrabilidad).

Mbps

Abreviatura de megabits por segundo, que es una velocidad de transferencia de datos.

MIB

Abreviatura de Management Information Base (base de información de administración).

MII

Abreviatura de Media Independent Interface (interfaz independiente de medios).

NAS

Abreviatura de Network Attached Storage (almacenamiento conectado a red).

NIC

Abreviatura de Network Interface Card (tarjeta de interfaz de red). Placa adaptadora de circuitos instalada en un equipo para brindar una conexión física con la red.

OID

Abreviatura de Object Identifiers (identificadores de objeto).

PCI

Abreviatura de Peripheral Component Interconnect (interconexión de componentes periféricos), que es una interfaz y tecnología de bus estándar para la conexión de periféricos a un sistema y para la comunicación con esos periféricos.

POST

Sigla de Power-On Self-Test (autoprueba de encendido), que es una secuencia de pruebas de diagnóstico que un sistema ejecuta automáticamente cuando se enciende.

PPP

Abreviatura de Point-to-Point Protocol (protocolo punto a punto), que es el protocolo estándar de Internet para transmitir datagramas de la capa de red (como paquetes IP) sobre vínculos punto a punto en serie.

RAC

Abreviatura de Remote Access Controller (controlador de acceso remoto).

RAM

Sigla de Random-Access Memory (memoria de acceso aleatorio). La RAM es una memoria de propósito general que se puede leer y en la que se puede escribir en los sistemas y en el iDRAC6.

redirección de consola

La redirección de consola es una función que envía la imagen de la pantalla, las funciones del ratón y las funciones del teclado de un servidor administrado a los dispositivos correspondientes en una estación de administración. Después puede usar la consola del sistema de la estación de administración para controlar el servidor administrado.

registro de hardware

Registra los eventos generados por el iDRAC6.

reversión

Para revertir a una versión anterior de software o firmware.

ROM

Sigla de Read-Only Memory (memoria de sólo lectura), que es la memoria desde la cual es posible leer los datos, pero no se pueden escribir en ella.

RPM

Abreviatura de Red Hat® Package Manager (administrador de paquetes Red Hat), que es un sistema de administración de paquetes para el sistema operativo Red Hat Enterprise Linux® que ayuda con la instalación de paquetes de software. Es similar a un programa de instalación.

SAC

Sigla de Special Administration Console (consola de administración especial) de Microsoft.

SAP

Abreviatura de Service Access Point (punto de acceso de servicio).

SEL

Sigla de System Event Log (registro de eventos del sistema).

servidor administrado

El servidor administrado es el sistema al que está incorporado el iDRAC6.

sistema administrado

Un sistema que está supervisado por una estación de administración se llama sistema administrado.

SM-CLP

Abreviatura de Server Management-Command Line Protocol (protocolo de línea de comandos para la administración de servidores). SM-CLP es un subcomponente de la iniciativa de SMASH supervisado por DMTF para una administración efectiva del servidor en varias plataformas. La especificación SM-CLP, junto con la especificación de direccionamiento de elemento administrado y varios perfiles en las especificaciones de asignación de SM-CLP, describe los destinos y verbos estandarizados para distintas ejecuciones de tareas de administración.

SMI

Abreviatura de Systems Management Interrupt (interrupción de administración del sistema).

SMTP

Abreviatura de Simple Mail Transfer Protocol (protocolo simple de transferencia de correo), que un protocolo utilizado para transferir el correo electrónico entre sistemas, por lo general a través de Ethernet.

SMWG

Abreviatura de Systems Management Working Group (grupo de trabajo de administración de sistemas).

SSH

Abreviatura de Secure Shell.

SSL

Abreviatura de Secure Sockets Layer (capa de sockets seguros).

TAP

Abreviatura de Telelocator Alphanumeric Protocol (protocolo alfanumérico de telelocalizador), que es un protocolo usado para enviar solicitudes a un servicio de localizador.

TCP/IP

Abreviatura de Transmission Control Protocol/Internet Protocol (protocolo de control de transmisiones/protocolo de Internet), que representa el conjunto de protocolos de Ethernet estándares que incluyen los protocolos de capa de red y capa de transporte.

TFTP

Abreviatura de Trivial File Transfer Protocol (protocolo trivial de transferencia de archivos), que es un protocolo de transferencia simple de archivos usado para descargar código de inicio a los dispositivos o sistemas sin discos.

Unified Server Configurator

Dell Unified Server Configurator es una utilidad de configuración incorporada que habilita sistemas y tareas de administración de almacenamiento desde un entorno incorporado a lo largo del ciclo de vida del sistema.

UPS

Abreviatura de Uninterruptible Power Supply (sistema de alimentación ininterrumpida).

USB

Abreviatura de bus serial universal.

USC

Abreviación de Unified Server Configurator.

UTC

Abreviatura de Universal Coordinated Time (tiempo universal coordinado). *Consulte* GMT.

VLAN

Abreviatura de Virtual Local Area Network (red virtual de área local).

VNC

Abreviatura de Virtual Network Computing (cómputo de red virtual).

VT-100

Abreviatura de Video Terminal 100 (terminal de video 100), que se usa en los programas de emulación de terminal más comunes.

WAN

Abreviatura de Wide Area Network (red de área amplia).

WS-MAN

Abreviatura del protocolo de servicios web para administración (WS-MAN:Web Services for Management). WS-MAN es un mecanismo de transporte para intercambio de información. WS-MAN ofrece un idioma universal para que los dispositivos puedan compartir datos, de forma que se puedan administrar más fácilmente.

Regresar a la página de contenido

Regresar a la página de contenido

Generalidades de los subcomandos de RACADM

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección contiene descripciones de los subcomandos que están disponibles en la interfaz de línea de comandos de RACADM.

PRECAUCIÓN: Racadm establece el valor de los objetos sin ejecutar funciones de validación. Por ejemplo, RACADM permite definir el valor del objeto validación de certificados en 1 con el objeto Active Directory en 0, aunque la validación de certificados sólo se realizará si Active Directory® está activado. De manera similar, el objeto cfgADSSOEnable puede definirse con el valor 0 ó 1 aun si el valor del objeto cfgADEnable es 0, aunque esta configuración sólo tendrá efecto si Active Directory está activado.

---

help

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-1 describe el comando **help**.

Tabla A-1. Comando help

Comando	Definición
help	Muestra una lista de todos los subcomandos disponibles para usar con **RACADM** y proporciona una breve descripción de cada uno.

Sinopsis

```
racadm help

racadm help <subcomando>
```

Descripción

El subcomando **help** muestra una lista de todos los subcomandos que están disponibles cuando se utiliza el comando **racadm** junto con una descripción de una línea. También puede escribir un subcomando después de **help** para que aparezca la sintaxis del subcomando específico.

Salida

El comando **racadm help** muestra una lista completa de subcomandos.

El comando **racadm help** <*subcomando*> muestra únicamente la información del subcomando especificado.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

arp

NOTA: Para usar este comando, debe tener permiso para **Ejecutar comandos de diagnóstico**.

La Tabla A-2 describe el comando **arp**.

Tabla A-2. Comando arp

Comando	Definición
arp	Muestra el contenido de la tabla ARP. Los registros de la tabla ARP no se pueden agregar ni eliminar.

Sinopsis

```
racadm arp
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

clearasrscreen

NOTA: Para usar este comando, debe tener permiso para **Borrar registros**.

La Tabla A-3 describe el subcomando **clearasrscreen**.

Tabla A-3. clearasrscreen

Subcomando	Definición
clearasrscreen	Borra de la memoria la pantalla del último bloqueo.

Sinopsis

```
racadm clearasrscreen
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

config

NOTA: Para usar el comando **getconfig**, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-4 describe los subcomandos **config** y **getconfig**.

Tabla A-4. config / getconfig

Subcomando	Definición
config	Configura el iDRAC6.
getconfig	Obtiene la información de configuración del iDRAC6.

Sinopsis

```
racadm config [-c|-p] -f <nombre_de_archivo>

racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> [-i <índice>] <valor>
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

Descripción

El subcomando **config** permite al usuario establecer parámetros de configuración del iDRAC6 individualmente o procesarlos en lote como parte de un archivo de configuración. Si la información es diferente, el objeto iDRAC6 se escribe con los nuevos valores.

Entrada

La Tabla A-5 describe las opciones del subcomando **config**.

NOTA: Las opciones **-f** y **-p** no se admiten en la consola en serie, Telnet o SSH.

Tabla A-5. Opciones y descripciones del subcomando config

Opción	Descripción
-f	La opción **-f** <***nombre_de_archivo***> hace que **config** lea el contenido del archivo especificado con el <***nombre_de_archivo***> y que configure el iDRAC6. El archivo debe contener los datos en el formato que se especifica en "Reglas del análisis".
-p	La opción **-p**, u opción de contraseña, hace que **config** elimine las anotaciones de contraseña que contiene el archivo de configuración **-f** ***<nombre_de_archivo>*** después de terminar la configuración.
-g	La opción -**g** ***<nombre_de_grupo>***, u opción de grupo, se debe usar con la opción **-o**. El <*nombre_de_grupo*> especifica el grupo que contiene al objeto que se va a definir.
-o	La opción **-o** ***<nombre_de_objeto>*** ***<valor>***, u opción de objeto, se debe usar con la opción **-g**. Esta opción especifica el nombre de objeto que se escribe con la cadena <*valor*>.
-i	La opción **-i** ***<índice>***, u opción de índice, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. El <*índice*> es un número entero decimal de 1 a 16. El índice se especifica aquí mediante el valor del índice; no mediante un valor asignado.
-c	La opción **-c**, u opción de verificación, se usa con el subcomando **config** y permite que el usuario analice el archivo **.cfg** en busca de errores de sintaxis. Si se encuentran errores, se mostrará el número de línea y una breve descripción de lo que está incorrecto. No se realizan las operaciones de escritura en el iDRAC6. Esta opción es sólo una revisión.

Salida

Este subcomando genera un mensaje de error cuando encuentra cualquiera de los siguientes problemas:

- Sintaxis, nombre de grupo, nombre de objeto o índice no válidos, u otros miembros no válidos de la base de datos.
- Fallas de la interfaz de línea de comandos de RACADM

Este subcomando indica cuántos objetos de configuración se escribieron y la cantidad total de objetos que había en el archivo **.cfg**.

Ejemplos

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

  Asigna el valor 10.35.10.110 al parámetro (objeto) de configuración **cfgNicIpAddress**. Este objeto de dirección IP está contenido en el grupo **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Configura o vuelve a configurar el iDRAC6. El archivo **myrac.cfg** se puede crear a partir del comando **getconfig**. El archivo **myrac.cfg** también se puede editar manualmente siempre y cuando se sigan las reglas de sintaxis.

  NOTA: El archivo **myrac.cfg** no contiene información de contraseña. Para incluir esta información en el archivo, se debe introducir manualmente. Si desea eliminar la información de contraseña del archivo **myrac.cfg** durante la configuración, utilice la opción **-p**.

---

getconfig

Descripción del subcomando getconfig

El subcomando **getconfig** permite al usuario recuperar parámetros de configuración del iDRAC6 individualmente, o se pueden recuperar todos los grupos de configuración y guardarse en un archivo.

Entrada

La Tabla A-6 describe las opciones del subcomando **getconfig**.

NOTA: Al utilizar la opción **-f** sin especificar un archivo, aparecerá el contenido del archivo en la pantalla de la terminal.

Tabla A-6. Opciones del subcomando getconfig

Opción	Descripción
-f	La opción **-f** <***nombre_de_archivo***> indica a getconfig que escriba toda la configuración del iDRAC6 en un archivo de configuración. Este archivo se puede usar para las operaciones de configuración en lote con el subcomando **config**. **NOTA:** La opción **-f** no crea registros para los grupos **cfgIpmiPet** y **cfgIpmiPef**. Usted debe establecer al menos un destino de excepción para capturar el grupo **cfgIpmiPet** en el archivo.
-g	La opción **-g <*nombre_de_grupo*>** u opción de **grupo** se puede usar para mostrar la configuración de un solo grupo. El **nombre_de_grupo** es el nombre del grupo que se utiliza en los archivos **racadm.cfg**. Si el grupo es un grupo indexado, use la opción **-i**.
-h	La opción **-h**, u opción de **ayuda**, muestra una lista de todos los grupos de configuración disponibles que se pueden utilizar. Esta opción es útil cuando usted no recuerda los nombres exactos de los grupos.
-i	La opción **-i <*índice*>**, u opción de **índice**, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. El <*índice*> es un número entero decimal de 1 a 16. Si no se especifica **-i <*índice*>**, se asumirá el valor de 1 para los grupos, que son tablas con varios registros. El índice se especifica mediante el valor del índice, no mediante un valor asignado.
-o	La opción -o **<*nombre_de_objeto*>**, u opción de objeto, especifica el nombre de objeto que se utiliza en la consulta. Esta opción es optativa y se puede utilizar con la opción -g.
-u	La opción **-u <*nombre de usuario*>**, u opción de **nombre de usuario**, se puede usar para mostrar la configuración del usuario especificado. La opción de **<*nombre_de_usuario*>** es el nombre de inicio de sesión del usuario.
-v	La opción **-v** muestra detalles adicionales en la pantalla de propiedades y se utiliza con la opción **-g**.

Salida

Este subcomando genera una salida de error cuando se encuentra cualquiera de los siguientes problemas:

- Sintaxis, nombre de grupo, nombre de objeto o índice no válidos, u otros miembros no válidos de la base de datos
- Fallas de transporte de la interfaz de línea de comandos de RACADM

Si no se encuentran errores, este subcomando muestra el contenido de la configuración especificada.

Ejemplos

- `racadm getconfig -g cfgLanNetworking`

  Muestra todas las propiedades de configuración (objetos) que se encuentran en el grupo **cfgLanNetworking**.

- `racadm getconfig -f myrac.cfg`

  Guarda todos los objetos de configuración de grupo del iDRAC6 en el archivo **myrac.cfg**.

- `racadm getconfig -h`

  Muestra una lista de los grupos de configuración disponibles en el iDRAC6.

- `racadm getconfig -u root`

  Muestra las propiedades de configuración del usuario root.

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  Muestra la instancia del grupo de usuario en el índice 2 con información detallada de los valores de propiedad.

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>

racadm getconfig -g <nombre_de_grupo> [-i <índice>]

racadm getconfig -u <nombre_de_usuario>

racadm getconfig -h
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

coredump

NOTA: Para usar este comando, debe tener permiso para **Ejecutar comandos de depuración**.

La Tabla A-7 describe el subcomando **coredump**.

Tabla A-7. coredump

Subcomando	Definición
coredump	Muestra el último volcado central del iDRAC6.

Sinopsis

```
racadm coredump
```

Descripción

El subcomando **coredump** muestra la información detallada que se relaciona con los problemas críticos recientes que hayan surgido con el RAC. La información de volcado de núcleo se puede usar para diagnosticar estos problemas críticos.

Si está disponible, la información de volcado de núcleo permanece después de ciclos de encendido del iDRAC6 y seguirá disponible hasta que se presente alguna de las condiciones siguientes:

- La información de volcado de núcleo se borra con el subcomando **coredumpdelete**.
- Se presenta otra condición crítica en el RAC. En este caso, la información de volcado de núcleo se referirá al último error crítico que se haya presentado.

Consulte el subcomando **coredumpdelete** para obtener más información acerca de cómo borrar el **volcado de núcleo**.

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

coredumpdelete

NOTA: Para usar este comando, se debe tener permiso para **Borrar registros** o **Ejecutar comandos de depuración**.

La Tabla A-8 describe el subcomando **coredumpdelete**.

Tabla A-8. coredumpdelete

Subcomando	Definición
coredumpdelete	Borra el volcado de núcleo almacenado en el iDRAC6.

Sinopsis

```
racadm coredumpdelete
```

Descripción

El subcomando **coredumpdelete** se puede usar para borrar los datos de **volcado de núcleo** que residan en ese momento en el RAC.

NOTA: Si se ejecuta un comando **coredumpdelete** y no hay un volcado de núcleo almacenado en el RAC en ese momento, el comando mostrará un mensaje de ejecución correcta. Este comportamiento es normal.

Consulte el subcomando **coredump** para obtener más información sobre cómo ver un volcado de núcleo.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

fwupdate

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC6**.

NOTA: Antes de comenzar la actualización del firmware, consulte "Configuración avanzada del iDRAC6" para obtener más información.

La Tabla A-9 describe el subcomando **fwupdate**.

Tabla A-9. fwupdate

Subcomando	Definición
fwupdate	Actualiza el firmware del iDRAC6

Sinopsis

```
racadm fwupdate -s

racadm fwupdate -g -u -a <dirección_IP_del_servidor_TFTP> [-d <ruta_de_acceso>]

racadm fwupdate -p -u -d <ruta_de_acceso>

racadm fwupdate -r
```

Descripción

El subcomando **fwupdate** permite que los usuarios actualicen el firmware del iDRAC6. El usuario puede:

- Revisar el estado del proceso de actualización del firmware
- Actualizar el firmware del iDRAC6 de un servidor TFTP si se proporciona una dirección IP y una ruta de acceso opcional
- Actualizar el firmware del iDRAC6 desde el sistema local de archivos por medio de RACADM local
- Reversión al firmware en espera

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

Entrada

La Tabla A-10 describe las opciones del subcomando **fwupdate**.

NOTA: La opción **-p** sólo se admite en la RACADM local y no se admite con las consolas serie, Telnet o SSH ni con las consolas remotas. Además, la opción **-p** no se admite en los sistemas operativos Linux.

Tabla A-10. Opciones del subcomando fwupdate

Opción	Descripción
-u	La opción **actualizar** ejecuta una suma de comprobación del archivo de actualización del firmware y comienza el verdadero proceso de actualización. Esta opción se puede usar junto con las opciones **-g** o **-p**. Al final de la actualización, el iDRAC6 realiza un restablecimiento ordenado.
-s	La opción **estado** muestra el estado actual del avance del proceso de actualización. Esta opción siempre se usa sin otras opciones.
-g	La opción **obtener** hace que el firmware obtenga el archivo de actualización del servidor TFTP. El usuario también debe especificar las opciones **-a** y **-d**. A falta de la opción **-a**, se leen los valores predeterminados de las propiedades que se encuentran en el grupo **cfgRemoteHosts** y se utilizan las propiedades **cfgRhostsFwUpdateIpAddr** y **cfgRhostsFwUpdatePath**.
-a	La opción **Dirección IP** especifica la dirección IP del servidor TFTP.
-d	La opción **-d**, u opción de **directorio**, especifica el directorio en el servidor TFTP o en el servidor del host del iDRAC6 donde reside el archivo de actualización del firmware.
-p	La opción **-p**, u opción de **colocar**, se utiliza para actualizar el archivo de firmware del iDRAC6 a partir del sistema administrado. La opción **-u** se debe usar con la opción **-p**.
-r	La opción **reversión** se usar para realizar una reversión hasta el firmware en espera.

Salida

Muestra un mensaje que indica qué operación se está ejecutando.

Ejemplos

- `racadm fwupdate -g -u - a 143.166.154.143 -d <ruta_de_acceso>`

  En este ejemplo, la opción **-g** hace que el firmware descargue el archivo de actualización de firmware de una ubicación (que se especifica con la opción **-d**) en el servidor TFTP en una dirección IP específica (que se indica con la opción **-a**). Después de que el archivo de imagen se descarga del servidor TFTP, el proceso de actualización comienza. Al terminar, el iDRAC6 se restablece.

- `racadm fwupdate -s`

  Esta opción lee el estado actual de la actualización de firmware.

- `racadm fwupdate -p -u -d <ruta_de_acceso>`

  En este ejemplo, la imagen de firmware para la actualización la proporciona el sistema de archivos del host.

NOTA: La opción **-p** no se admite en la interfaz RACADM remota para el subcomando fwupdate. La actualización del firmware mediante RACADM remoto a través de la ruta de acceso local no se admite en los sistemas operativos Linux.

---

getssninfo

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-11 describe el subcomando **getssninfo**.

Tabla A-11. Subcomando getssninfo

Subcomando	Definición
getssninfo	Recupera información de la sesión para una o más sesiones activas o pendientes desde la tabla de sesiones del administrador de sesiones.

Sinopsis

```
racadm getssninfo [-A] [-u <nombre_de_usuario> | *]
```

Descripción

El comando **getssninfo** muestra una lista de los usuarios que están conectados al iDRAC6. La información de resumen proporciona la siguiente información:

- Nombre de usuario
- Dirección IP (si se aplica)
- Tipo de sesión (por ejemplo, serie o Telnet)
- Consolas en uso (por ejemplo, medios virtuales o KVM virtual)

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

Entrada

La Tabla A-12 describe las opciones del subcomando **getssninfo**.

Tabla A-12. Opciones del subcomando getssninfo

Opción	Descripción
-A	La opción **-A** elimina la impresión de los encabezados de los datos.
-u	La opción **-u <nombre de usuario>** limita el mensaje impreso de salida a sólo los registros detallados de la sesión para el nombre de usuario proporcionado. Si se proporciona un símbolo "*" como el nombre de usuario, se enumeran todos los usuarios. La información de resumen no aparecerá cuando se especifique esta opción.

Ejemplos

- `racadm getssninfo`

La Tabla A-13 ofrece un ejemplo del mensaje de salida del comando **racadm getssninfo**.

Tabla A-13. Ejemplo del mensaje de salida del subcomando getssninfo

Usuario	Dirección IP	Tipo	Consolas
root	192.168.0.10	Telnet	KVM virtual

- `racadm getssninfo -A`

  `"root" "143.166.174.19" "Telnet" "NONE"("NINGUNO")`

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "NINGUNO"`

  `"bob" "143.166.174.19" "GUI" "NINGUNO"`

getsysinfo

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-14 describe el subcomando **racadm getsysinfo**.

Tabla A-14. getsysinfo

Comando	Definición
getsysinfo	Muestra información del iDRAC6, información del sistema e información del estado de la vigilancia.

Sinopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6] [-r]
```

Descripción

El subcomando **getsysinfo** muestra información relacionada con el RAC, el sistema administrado y la configuración de la vigilancia.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

Entrada

La Tabla A-15 describe las opciones del subcomando **getsysinfo**.

Tabla A-15. Opciones del subcomando getsysinfo

Opción	Descripción
4	Muestra la configuración de IPv4
6	Muestra la configuración de IPv6
-c	Muestra la configuración común
-d	Muestra la información del iDRAC6
-s	Muestra la información del sistema
-w	Muestra la información de vigilancia
-A	Elimina la impresión de encabezados/etiquetas

Si la opción **-w** no se especifica, las demás opciones se utilizarán como valores predeterminados.

Salida

El subcomando **getsysinfo** muestra información relacionada con el RAC, el sistema administrado y la configuración de la vigilancia.

Ejemplo del mensaje de salida

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
Hardware Version = 0.01
```

```
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
DNS RAC Name = iDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig              = 1
DNS Server from DHCPv6  = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::

System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON

Watchdog Information:
Recovery Action = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

Ejemplos

- `racadm getsysinfo -A -s`

  ```
  "System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

  "Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"

  ("Información del sistema:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Nombre de host"

  "Microsoft Windows 2000 versión 5.0, número de compilación 2195, Service Pack 2" "Encendido")
  ```

- `racadm getsysinfo -w -s`

```
System Information:
System Model            = PowerEdge 2900
System BIOS Version     = 0.2.3
BMC Firmware Version    = 0.17
Service Tag             = 48192
Host Name               = racdev103
OS Name                 = Microsoft Windows Server 2003
Power Status            = OFF


Watchdog Information:
Recovery Action         = None
Present countdown value  = 0 seconds
Initial countdown value = 0 seconds
```

Restricciones

Los campos Nombre de host y Nombre del sistema operativo en el mensaje de salida de **getsysinfo** mostrarán información correcta sólo si el software de sistemas Dell™ OpenManage™ está instalado en el sistema administrado. Si OpenManage no está instalado en el sistema administrado, es posible que estos campos estén vacíos o tengan información incorrecta..

---

getractime

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-16 describe el subcomando **getractime**.

Tabla A-16. getractime

Subcomando	Definición
getractime	Muestra la hora actual del controlador de acceso remoto.

Sinopsis

```
racadm getractime [-d]
```

Descripción

Cuando se usa sin opciones, el subcomando **getractime** muestra la hora en formato común legible.

Con la opción **-d**, **getractime** muestra la hora en formato, *aaaammddhhmmss.mmmmmms*, que es el mismo formato que genera el comando **date** de UNIX.

Salida

El subcomando **getractime** muestra el mensaje de salida en una línea.

Ejemplo del mensaje de salida

```
racadm getractime

Thu Dec 8 20:15:26 2005 (Jue 8 de dic 20:15:26 2005)

racadm getractime -d

20051208201542.000000
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

ifconfig

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de diagnóstico** o para **Configurar el iDRAC**.

La Tabla A-17 describe el subcomando **ifconfig**.

Tabla A-17. ifconfig

Subcomando	Definición
ifconfig	Muestra el contenido de la tabla de interfaz de red.

Sinopsis

```
racadm ifconfig
```

---

netstat

NOTA: Para usar este comando, debe tener permiso para **Ejecutar comandos de diagnóstico**.

La Tabla A-18 describe el subcomando **netstat**.

Tabla A-18. netstat

Subcomando	Definición
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.

Sinopsis

```
racadm netstat
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

ping

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de diagnóstico** o para **Configurar el iDRAC**.

La Tabla A-19 describe el subcomando **ping**.

Tabla A-19. ping

Subcomando	Definición
ping	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IP de destino. Un paquete de eco de ICMP se envía a la dirección IP de destino en función del contenido de tabla de enrutamiento actual.

Sinopsis

```
racadm ping <dirección_IP>
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

setniccfg

NOTA: Para usar el comando **setniccfg**, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-20 describe el subcomando **setniccfg**.

Tabla A-20. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

NOTA: Los términos tarjeta de interfaz de red y puerto de administración de Ethernet pueden usarse como sinónimos.

Sinopsis

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <dirección_IPv4> <máscara_de_red> <puerta_de_enlace IPv4>

racadm setniccfg -s6 <dirección_IPv6> <longitud_del_prefijo_IPv6> <puerta_de_enlace_IPv6>

racadm setniccfg -o
```

Descripción

El subcomando **setniccfg** establece la dirección IP del controlador.

- La opción **-d** activa DHCP para el puerto de administración de Ethernet (el valor predeterminado es DHCP desactivado).
- La opción **-d6** activa AutoConfig para el puerto de administración de Ethernet. Está activado de manera predeterminada.
- La opción **-s** activa la configuración de IP estática. Se pueden especificar la dirección IPv4, la máscara de red y la puerta de enlace. De lo contrario, se usa la configuración estática existente. <*dirección_IPv4*>, <*máscara_de_red*> y <*puerta_de_enlace*> se deben escribir como cadenas separadas con puntos.
- La opción **-s6** activa la configuración de IPv6 estática. Se pueden especificar la dirección IPv6, la longitud del prefijo y la puerta de enlace IPv6.
- La opción **-o** desactiva completamente el puerto de administración de Ethernet.

Salida

Si la operación no es satisfactoria, el subcomando **setniccfg** muestra el mensaje de error correspondiente. Si es satisfactoria, aparecerá un mensaje.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

getniccfg

NOTA: Para usar el comando **getniccfg**, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-21 describe los subcomandos **setniccfg** y **getniccfg**.

Tabla A-21. setniccfg / getniccfg

Subcomando	Definición
getniccfg	Muestra la configuración IP actual del controlador.

Sinopsis

```
racadm getniccfg
```

Descripción

El subcomando **getniccfg** muestra la configuración actual del puerto de administración de Ethernet.

Ejemplo del mensaje de salida

Si la operación no es satisfactoria, el subcomando **getniccfg** muestra el mensaje de error correspondiente. De lo contrario, cuando se ejecute

satisfactoriamente, el mensaje aparecerá en el formato siguiente:

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1

(NIC activado     = 1

DHCP activado    = 1

Dirección IP      = 192.168.0.1

Máscara de subred     = 255.255.255.0

Puerta de enlace         = 192.168.0.1)
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

getsvctag

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-22 describe el subcomando **getsvctag**.

Tabla A-22. getsvctag

Subcomando	Definición
getsvctag	Muestra la etiqueta de servicio.

Sinopsis

```
racadm getsvctag
```

Descripción

El subcomando **getsvctag** muestra la etiqueta de servicio del sistema host.

Ejemplo

Escriba getsvctag en la petición de comandos. El mensaje de salida es como el siguiente:

```
Y76TP0G
```

El comando muestra `0` cuando se ejecuta satisfactoriamente y valores distintos de cero cuando hay errores.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

racdump

NOTA: Para usar este comando, debe tener permiso para **Depurar**.

La Tabla A-23 describe el subcomando **racdump**.

Tabla A-23. racdump

Subcomando	Definición
racdump	Muestra información general y del estado del iDRAC6.

Sinopsis

```
racadm racdump
```

Descripción

El subcomando **racdump** proporciona un solo comando para obtener el volcado, el estado e información general de la tarjeta del iDRAC6.

Al procesar el subcomando **racdump**, aparece la siguiente información:

- Información general del sistema/RAC
- Volcado de núcleo
- Información de la sesión
- Información del proceso
- Información de la compilación de firmware

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

racreset

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-24 describe el subcomando **racreset**.

Tabla A-24. racreset

Subcomando	Definición
racreset	Restablece el iDRAC6.

NOTA: Cuando se ejecuta un subcomando racreset, es posible que el iDRAC6 tarde hasta un minuto para volver a un estado utilizable.

Sinopsis

```
racadm racreset [hard | soft]
```

Descripción

El subcomando **racreset** realiza un restablecimiento del iDRAC6. El evento de restablecimiento se escribe en el registro del iDRAC6.

El restablecimiento forzado realiza una operación de restablecimiento profundo en el RAC. El restablecimiento forzado sólo se debe realizar como último recurso para recuperar el RAC.

NOTA: Se debe reiniciar el sistema después de ejecutar un restablecimiento forzado del iDRAC6, conforme se describe en la Tabla A-25.

La Tabla A-25 describe las opciones del subcomando **racreset**.

Tabla A-25. Opciones del subcomando racreset

Opción	Descripción
hard	El restablecimiento *forzado* realiza una operación de restablecimiento profundo en el controlador de acceso remoto. El restablecimiento forzado sólo se debe utilizar como último recurso para restablecer el controlador iDRAC6 para fines de recuperación.
soft	Un restablecimiento *ordenado* ejecuta una operación de reinicio ordenado en el RAC.

Ejemplos

- `racadm racreset`

  Inicia la secuencia de restablecimiento ordenado del iDRAC6.

- `racadm racreset hard`

  Inicia la secuencia de restablecimiento forzado del iDRAC6.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

racresetcfg

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-26 describe el subcomando **racresetcfg**.

Tabla A-26. racresetcfg

Subcomando	Definición
racresetcfg	Restablece los valores predeterminados de fábrica de toda la configuración del iDRAC6.

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

Descripción

El comando **racresetcfg** quita todos los registros de propiedad de la base de datos que hayan sido configurados por el usuario. La base de datos tiene propiedades predeterminadas para todos los registros que se usan para restablecer el controlador a sus valores predeterminados originales. El iDRAC6 se restablece automáticamente después de restablecer las propiedades de la base de datos.

NOTA: Este comando elimina la configuración actual del iDRAC6 y restablece los valores predeterminados originales de la configuración serie y del iDRAC6. Tras el restablecimiento, el nombre y la contraseña predeterminados son **root** y **calvin**, respectivamente, y la dirección IP es 192.168.0.120. Si ejecuta un comando **racresetcfg** desde un cliente de la red (por ejemplo, un explorador web admitido, RACADM remota, Telnet o SSH), deberá usar la

dirección IP predeterminada.

NOTA: Algunos procesos de firmware del iDRAC6 deben detenerse y reiniciarse para restablecer todos los valores predeterminados. El iDRAC6 dejará de responder durante alrededor de 30 segundos mientras se completa esta operación.

---

serveraction

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de control del servidor**.

La Tabla A-27 describe el subcomando **serveraction**.

Tabla A-27. serveraction

Subcomando	Definición
serveraction	Ejecuta un restablecimiento del sistema administrado o un ciclo de encendido y apagado.

Sinopsis

```
racadm serveraction <acción>
```

Descripción

El subcomando serveraction permite que los usuarios realicen operaciones de administración de energía en el sistema host. La Tabla A-28 describe las opciones de control de alimentación de **serveraction**.

Tabla A-28. Opciones del subcomando serveraction

Cadena	Definición
<*acción*>	Especifica la acción. Las opciones para la cadena <*acción*> son: • **powerdown**: apaga el sistema administrado. • **powerup**: enciende el sistema administrado. • **powercycle**: ejecuta una operación de ciclo de encendido en el sistema administrado. Esta acción es similar a la acción de presionar el botón de encendido en el panel frontal del sistema para apagarlo y después encender el sistema. • **powerstatus**: muestra el estado actual de la alimentación del servidor ("Encendido" o "Apagado") • **hardreset**: ejecuta una operación de restablecimiento (reinicio) en el sistema administrado.

Salida

El subcomando **serveraction** mostrará un mensaje de error si la operación solicitada no puede ejecutarse o un mensaje de ejecución satisfactoria si la operación terminó de manera satisfactoria.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

getraclog

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-29 describe el comando **racadm getraclog**.

Tabla A-29. getraclog

Comando	Definición

getraclog -i	Muestra la cantidad de entradas del registro del iDRAC6.
getraclog	Muestra las entradas del registro del iDRAC6.

Sinopsis

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c número] [-s entrada_de_inicio] [-m]
```

Descripción

El comando **getraclog -i** muestra el número de entradas en el registro del iDRAC6.

Las siguientes opciones permiten que el comando **getraclog** lea las entradas:

- **-A**: muestra el mensaje de salida sin encabezados ni etiquetas.
- **-c**: informa el número máximo de entradas que se mostrarán.
- **-m**: muestra una pantalla informativa a la vez y pregunta al usuario antes de continuar (parecido al comando **more** de UNIX).
- **-o**: muestra el mensaje de salida en una sola línea.
- **-s**: especifica la entrada inicial que se utilizará en los resultados.

NOTA: Si no se introducen opciones, se mostrará todo el registro.

Salida

El mensaje de salida predeterminado muestra el número de entrada, la fecha y la hora, el origen y la descripción. La fecha y hora comienza a la media noche del 1.º de enero y continúa hasta que el sistema se inicia. Después del inicio del sistema, se utiliza la fecha y hora del sistema.

Ejemplo del mensaje de salida

```
Record:       1
Date/Time:    Dec 8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103 (Entrada:       1
Fecha y hora:    8 de dic 08:10:11
Origen:       inicio de sesión[433]
Descripción:  inicio de sesión de root desde 143.166.157.1030
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

clrraclog

NOTA: Para usar este comando, debe tener permiso para **Borrar registros**.

Sinopsis

```
racadm clrraclog
```

Descripción

El subcomando **clrraclog** elimina todas las entradas existentes del registro del iDRAC6. Se crea una nueva entrada única para registrar la fecha y la hora en la que el registro fue borrado.

---

getsel

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-30 describe el comando **getsel**.

Tabla A-30. getsel

Comando	Definición
getsel -i	Muestra el número de entradas en el registro de eventos del sistema.
getsel	Muestra las entradas del registro de eventos del sistema.

Sinopsis

```
racadm getsel -i

racadm getsel [-E] [-R] [-A] [-o] [-c número] [-s número] [-m]
```

Descripción

El comando **getsel -i** muestra el número de entradas en el registro de eventos del sistema.

Las siguientes opciones **getsel** (sin la opción **-i**) se utilizan para leer entradas.

-A: muestra el mensaje de salida sin encabezados ni etiquetas.

-c: informa el número máximo de entradas que se mostrarán.

-o: muestra el mensaje de salida en una sola línea.

-s: especifica la entrada inicial que se utilizará en los resultados.

-E: coloca los 16 bytes del registro de eventos del sistema sin procesar al final de cada línea del mensaje de salida, como secuencia de valores hexadecimales.

-R: sólo se imprimen los datos sin procesar.

-m: muestra una pantalla a la vez y pregunta al usuario antes de continuar (parecido al comando **more** de UNIX).

NOTA: Si no se especifican argumentos, se mostrará todo el registro.

Salida

El mensaje de salida predeterminado muestra el número de entrada, la fecha y la hora, el origen y la descripción.

Por ejemplo:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted

(Entrada:       1
Fecha y hora:   16/11/05 22:40:43
Gravedad:    En buen estado
Descripción: Registro de eventos de la placa base: sensor de registro de eventos de la placa base, se confirmó que el registro fue borrado)
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

clrsel

NOTA: Para usar este comando, debe tener permiso para **Borrar registros**.

Sinopsis

```
racadm clrsel
```

Descripción

El comando **clrsel** quita todas las entradas existentes del registro de eventos del sistema (SEL).

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

gettracelog

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el iDRAC**.

La Tabla A-31 describe el subcomando **gettracelog**.

Tabla A-31. gettracelog

Comando	Definición
gettracelog -i	Muestra la cantidad de entradas del registro de rastreo del iDRAC6.
gettracelog	Muestra el registro de rastreo del iDRAC6.

Sinopsis

```
racadm gettracelog -i

racadm gettracelog [-A] [-o] [-c número] [-s entrada_inicial] [-m]
```

Descripción

El comando **gettracelog** (sin la opción **-i**) lee las entradas. Se utilizan las siguientes opciones de **gettracelog** para leer entradas:

-i: muestra el número de entradas que hay en el registro de rastreo del iDRAC6

-m: muestra una pantalla a la vez y pregunta al usuario antes de continuar (parecido al comando **more** de UNIX).

-o: muestra el mensaje de salida en una sola línea.

-c: especifica el número de entradas que se mostrarán

-s: especifica la entrada inicial que se mostrará

-A: no muestra encabezados ni etiquetas

Salida

El mensaje de salida predeterminado muestra el número de entrada, la fecha y la hora, el origen y la descripción. La fecha y hora comienza a la media noche del 1.° de enero y continúa hasta que el sistema se inicia. Después del inicio del sistema, se utiliza la fecha y hora del sistema.

Por ejemplo:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]
```

```
Description: root from 143.166.157.103: session timeout sid 0be0aef4


(Entrada: 1

Fecha y hora: 8 de dic 08:10:30

Origen: ssnmgrd[175]

Descripción: root desde 143.166.157.103: expiración de tiempo de la sesión sid 0be0aef4)
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

sslcsrgen

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-32 describe el subcomando **sslcsrgen**.

Tabla A-32. sslcsrgen

Subcomando	Descripción
sslcsrgen	Genera y descarga una solicitud de firma de certificado (CSR) SSL del RAC.

Sinopsis

```
racadm sslcsrgen [-g] [-f <nombre_de_archivo>]

racadm sslcsrgen -s
```

Descripción

El subcomando **sslcsrgen** se puede usar para generar una CSR y descargar el archivo en el sistema de archivos local del cliente. La CSR se puede utilizar para crear un certificado personalizado SSL que se puede usar para realizar transacciones SSL en el RAC.

Opciones

NOTA: La opción **-f** no se admite en la consola serie, Telnet o SSH.

La Tabla A-33 describe las opciones del subcomando **sslcsrgen**.

Tabla A-33. Opciones del subcomando sslcsrgen

Opción	Descripción
-g	Genera una nueva CSR.
-s	Muestra el estado del proceso de generación de la CSR (generación en progreso, activa o ninguna).
-f	Especifica el nombre de archivo de la ubicación, *<nombre_de_archivo>*, donde la CSR se va a descargar.

NOTA: Si no se especifica la opción **-f**, se asignará el nombre de archivo predeterminado de **sslcsr** en el directorio actual.

Si no se especifican opciones, se generará una CSR y se descargará en el sistema local de archivos como **sslcsr** de manera predeterminada. La opción **-g** no se puede usar con la opción **-s**, y la opción **-f** sólo se puede usar con la opción **-g**.

El subcomando **sslcsrgen -s** muestra uno de los siguientes códigos de estado:

- La CSR se generó de manera satisfactoria.

- La CSR no existe.
- Generación de la CSR en progreso.

Restricciones

El subcomando **sslcsrgen** sólo se puede ejecutar desde un cliente de RACADM local o remota y no se puede usar en la interfaz serie, Telnet o SSH.

NOTA: Antes de que se pueda generar una CSR, los campos de la misma se deben configurar en el grupo **cfgRacSecurity** de RACADM. Por ejemplo: racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName Mi_empresa

Ejemplos

```
racadm sslcsrgen -s
```

O bien:

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

sslcertupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-34 describe el subcomando **sslcertupload**.

Tabla A-34. sslcertupload

Subcomando	Descripción
sslcertupload	Carga un certificado de CA o de servidor SSL del cliente al RAC.

Sinopsis

```
racadm sslcertupload -t <tipo> [-f <nombre_de_archivo>]
```

Opciones

La Tabla A-35 describe las opciones del subcomando **sslcertupload**.

Tabla A-35. Opciones del subcomando sslcertupload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a cargar, ya sea el certificado CA o el certificado del servidor. 1 = certificado del servidor 2 = certificado de CA
-f	Especifica el nombre de archivo del certificado que se va a cargar. Si no se especifica el archivo, se seleccionará el archivo **sslcert** en el directorio actual.

El comando **sslcertupload** muestra `0` cuando se ejecuta de manera satisfactoria y un valor distinto a cero cuando no se ejecuta satisfactoriamente.

Restricciones

El subcomando **sslcertupload** sólo se puede ejecutar desde un cliente de RACADM local o remota. El subcomando **sslcsrgen** no se puede usar en la interfaz serie, Telnet o SSH.

Ejemplo

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertdownload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-36 describe el subcomando **sslcertdownload**.

Tabla A-36. sslcertdownload

Subcomando	Descripción
sslcertupload	Descarga un certificado SSL del iDRAC6 en el sistema de archivos del cliente.

Sinopsis

```
racadm sslcertdownload -t <tipo> [-f <nombre_de_archivo>]
```

Opciones

La Tabla A-37 describe las opciones del subcomando **sslcertdownload**.

Tabla A-37. Opciones del subcomando sslcertdownload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a descargar, ya sea un certificado de Microsoft® Active Directory® o un certificado de servidor. 1 = certificado del servidor 2 = certificado de Microsoft Active Directory
-f	Especifica el nombre de archivo del certificado que se va a cargar. Si no se especifica la opción **-f** o el nombre de archivo, se seleccionará el archivo **sslcert** en el directorio actual.

El comando **sslcertdownload** muestra `0` cuando se ejecuta de manera satisfactoria y un valor distinto a cero cuando no se ejecuta satisfactoriamente.

Restricciones

El subcomando **sslcertdownload** sólo se puede ejecutar desde un cliente de RACADM local o remota. El subcomando **sslcsrgen** no se puede usar en la interfaz serie, Telnet o SSH.

Ejemplo

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertview

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-38 describe el subcomando **sslcertview**.

Tabla A-38. sslcertview

Subcomando	Descripción
sslcertview	Muestra el servidor SSL o el certificado de CA que existe en el RAC.

Sinopsis

```
racadm sslcertview -t <tipo> [-A]
```

Opciones

La Tabla A-39 describe las opciones del subcomando **sslcertview**.

Tabla A-39. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado que se va a descargar, ya sea un certificado de Microsoft Active Directory o un certificado de servidor. 1 = certificado del servidor 2 = certificado de Microsoft Active Directory
-A	Evita la impresión de encabezados/etiquetas.

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Issuer Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Valid From                : Jul 8 16:21:56 2005 GMT
Valid To                  : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
```

```
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

sslkeyupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-40 describe el subcomando **sslkeyupload**.

Tabla A-40. sslkeyupload

Subcomando	Descripción
sslkeyupload	Carga una clave SSL del cliente al iDRAC6.

Sinopsis

```
racadm sslkeyupload -t <tipo> -f <nombre_de_archivo>
```

Opciones

La Tabla A-41 describe las opciones del subcomando **sslkeyupload**.

Tabla A-41. Opciones del subcomando sslkeyupload

Opción	Descripción
-t	Especifica la clave que se va a cargar. 1 = clave SSL que se usa para generar el certificado del servidor
-f	Especifica el nombre de archivo de la clave SSL que se cargará.

El comando **sslkeyupload** muestra `0` cuando se ejecuta de manera satisfactoria y un valor distinto a cero cuando no se ejecuta satisfactoriamente.

Restricciones

El subcomando **sslkeyupload** sólo se puede ejecutar desde un cliente de RACADM local o remota. No se puede usar en la interfaz serie, telnet ni SSH.

Ejemplo

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

Interfaces admitidas

- RACADM local
- RACADM remota

---

testemail

La Tabla A-42 describe el subcomando **testemail**.

Tabla A-42. Configuración de testemail

Subcomando	Descripción
testemail	Prueba la función de alertas por correo electrónico del RAC.

Sinopsis

```
racadm testemail -i <índice>
```

Descripción

Envía un correo electrónico de prueba del iDRAC6 a un destino especificado.

Antes de ejecutar el comando de correo electrónico de prueba, compruebe que el índice que se especifica en el grupo **cfgEmailAlert** de RACADM está habilitado y configurado correctamente. La Tabla A-43 muestra una lista y los comandos asociados con el grupo **cfgEmailAlert**.

Tabla A-43. Configuración de testemail

Acción	Comando
Activa la alerta	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Establece la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 usuario1@mi_empresa.com
Establece el mensaje personalizado que se envía a la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Ésta es una prueba"
Comprueba que la dirección IP SMTP esté configurada correctamente	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152
Muestra la configuración actual de las alertas por correo electrónico	racadm getconfig -g cfgEmailAlert -i *<índice>* donde *<índice>* es un número de 1 a 4

Opciones

La Tabla A-44 describe las opciones del subcomando **testemail**.

Tabla A-44. Subcomandos de testemail

Opción	Descripción
-i	Especifica el índice de la alerta por correo electrónico que se va a probar.

Salida

Ninguna.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

testtrap

NOTA: Para usar este comando, debe tener permiso para **Probar alertas**.

La Tabla A-45 describe el subcomando **testtrap**.

Tabla A-45. testtrap

Subcomando	Descripción
testtrap	Prueba la función de alertas de excepción SNMP del RAC.

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

El subcomando **testtrap** prueba la función de alertas de excepción SNMP del RAC mediante el envío de una captura de prueba del iDRAC6 a un destinatario de excepción determinado de la red.

Antes de ejecutar el subcomando **testtrap** compruebe que el índice especificado en el grupo **cfgIpmiPet** de RACADM esté configurado correctamente.

La Tabla A-46 muestra una lista y los comandos asociados con el grupo **cfgIpmiPet**.

Tabla A-46. Comandos de cfgEmailAlert

Acción	Comando
Activa la alerta	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
Establece la dirección IP de correo electrónico de destino	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
Muestra la configuración actual de la excepción de prueba	racadm getconfig -g cfgIpmiPet -i *<índice>* donde *<índice>* es un número de 1 a 4

Entrada

La Tabla A-47 describe las opciones del subcomando **testtrap**.

Tabla A-47. Opciones del subcomando testtrap

Opción	Descripción
-i	Especifica el índice de la configuración de excepción que se debe usar para la prueba. Los valores válidos son de 1 a 4.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

vmdisconnect

NOTA: Para usar este comando, se debe tener permiso de **Acceso a los medios virtuales**.

La Tabla A-48 describe el subcomando **vmdisconnect**.

Tabla A-48. vmdisconnect

Subcomando	Descripción
vmdisconnect	Cierra todas las conexiones de medios virtuales del iDRAC6 provenientes de clientes remotos.

Sinopsis

```
racadm vmdisconnect
```

Descripción

El subcomando **vmdisconnect** permite que el usuario desconecte la sesión de medios virtuales de otro usuario. Una vez desconectado, la interfaz web mostrará el estado correspondiente de la conexión. Esto sólo está disponible a través del uso de RACADM local o remota.

El subcomando **vmdisconnect** permite que un usuario del iDRAC6 pueda desconectar todas las sesiones activas de medios virtuales. Las sesiones activas de medios virtuales se pueden mostrar en la interfaz web del iDRAC6 o por medio del subcomando **getsysinfo** de RACADM.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

vmkey

NOTA: Para usar este comando, se debe tener permiso de **Acceso a los medios virtuales**.

La Tabla A-49 describe el subcomando **vmkey**.

Tabla A-49. vmkey

Subcomando	Descripción
vmkey	Realiza operaciones relacionadas con las memorias de medios virtuales.

Sinopsis

```
racadm vmkey <acción>
```

Si *<acción>* se configura como reset, se restablecerá el tamaño predeterminado de 256 MB de la memoria flash virtual.

Descripción

Al cargar una imagen personalizada de memoria de medios virtuales al RAC, el tamaño de la memoria será el tamaño de la imagen. El subcomando vmkey se puede usar para restablecer el tamaño original predeterminado de la memoria, que es de 256 MB en el iDRAC6.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

usercertupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-50 describe las opciones del subcomando **usercertupload**.

Tabla A-50. usercertupload

Subcomando	Descripción
usercertupload	Carga un certificado de usuario o un certificado de CA de usuario del cliente en el iDRAC6.

Sinopsis

```
racadm usercertupload -t <tipo> [-f <nombre_de_archivo>] -i <índice>
```

Opciones

La Tabla A-51 describe las opciones del subcomando **usercertupload**.

Tabla A-51. Opciones del subcomando usercertupload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a cargar, ya sea el certificado CA o el certificado del servidor. 1 = certificado de usuario 2 = certificado de CA de usuario
-f	Especifica el nombre de archivo del certificado que se va a cargar. Si no se especifica el archivo, se seleccionará el archivo **sslcert** en el directorio actual.
-i	Número de índice del usuario. Valores válidos: de 1 a 16

El comando **usercertupload** muestra `0` cuando se ejecuta de manera satisfactoria y un valor distinto a cero cuando no se ejecuta satisfactoriamente.

Restricciones

El subcomando **usercertupload** sólo se puede ejecutar desde un cliente de RACADM local o remota.

Ejemplo

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

Interfaces admitidas

- RACADM local
- RACADM remota

---

usercertview

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-52 describe el subcomando **usercertview**.

Tabla A-52. usercertview

Subcomando	Descripción
usercertview	Muestra el certificado de usuario o el certificado de CA de usuario que existe en el iDRAC6.

Sinopsis

```
racadm sslcertview -t <tipo> [-A] -i <índice>
```

Opciones

La Tabla A-53 describe las opciones del subcomando **sslcertview**.

Tabla A-53. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado que se mostrará; el certificado de usuario o el certificado de CA de usuario. 1 = certificado de usuario 2 = certificado de CA de usuario
-A	Evita la impresión de encabezados/etiquetas.
-i	Número de índice del usuario. Los valores válidos son de 1 a 16.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM Telnet/SSH/serie

---

localConRedirDisable

NOTA: Sólo un usuario de RACADM local puede ejecutar este comando.

La Tabla A-54 describe el subcomando **localConRedirDisable**.

Tabla A-54. localConRedirDisable

Subcomando	Descripción
localConRedirDisable	Desactiva la redirección de consola a la estación de administración.

Sinopsis

```
racadm localConRedirDisable <opción>
```

Si *<opción>* se establece como 1, se desactivará la redirección de consola..

Si *<opción>* se establece como 0, se activará la redirección de consola.

Interfaces admitidas

- RACADM local

---

krbkeytabupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC**.

La Tabla A-55 describe el subcomando **krbkeytabupload**.

Tabla A-55. krbkeytabupload

Subcomando	Descripción
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.

Sinopsis

```
racadm krbkeytabupload [-f <nombre de archivo>]
```

<nombre de archivo> es el nombre del archivo que incluye la ruta de acceso.

Opciones

La Tabla A-56 describe las opciones del subcomando **krbkeytabupload**.

Tabla A-56. Opciones del subcomando kerbkeytabupload

Opción	Descripción
-f	Especifica el nombre del archivo keytab a cargar. Si no se especifica el archivo, se seleccionará el archivo keytab que está en el directorio actual.

El comando **krbkeytabupload** muestra el valor `0` cuando se ejecuta de manera correcta, y un valor distinto de cero cuando no se ejecuta correctamente.

Restricciones

El subcomando **krbkeytabupload** sólo se puede ejecutar desde un cliente de RACADM local o remoto.

Ejemplo

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

Interfaces admitidas

- RACADM local
- RACADM remota

Regresar a la página de contenido

Regresar a la página de contenido

Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

La base de datos de propiedades del iDRAC6 contiene la información de configuración del iDRAC6. Los datos se organizan por objeto asociado y los objetos se organizan por grupos de objetos. Las identificaciones de los grupos y objetos admitidos por la base de datos de propiedades se enumeran en esta sección.

Use las identificaciones de objeto y grupo con la utilidad RACADM para configurar el iDRAC6. Las secciones siguientes describen cada objeto e indican si el objeto se puede leer, escribir o ambos.

PRECAUCIÓN: El comando Racadm establece el valor de los objetos sin ejecutar funciones de convalidación. Por ejemplo, RACADM permite definir el valor del objeto de validación de certificados en 1 y el objeto Active Directory en 0, aunque la validación de certificados sólo se realizará si Active Directory® está activado. De manera similar, el objeto cfgADSSOEnable puede definirse con el valor 0 ó 1 a pesar de que el valor del objeto cfgADEnable sea 0, aunque esta configuración sólo tendrá efecto si Active Directory está activado.

Todos los valores de cadena se limitan a los caracteres ASCII que se pueden mostrar en pantalla, salvo en los casos donde se indica lo contrario.

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#$%^&*()_+-={}[]|\:";'<>,.?/
```

---

idRacInfo

Este grupo contiene parámetros de la pantalla para proporcionar información acerca de las características específicas del iDRAC6 que se está consultando.

Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

idRacProductInfo (sólo lectura)

Valores legales

Una cadena de hasta 63 caracteres ASCII.

Predeterminado

Integrated Dell Remote Access Controller

Descripción

Una cadena de texto que identifica el producto.

idRacDescriptionInfo (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres ASCII.

Predeterminado

Este componente de sistema proporciona un conjunto completo de funciones de administración remota para los servidores Dell PowerEdge.

Descripción

Una descripción de texto del tipo del iDRAC.

idRacVersionInfo (sólo lectura)

Valores legales

Una cadena de hasta 63 caracteres ASCII.

Predeterminado

<número de versión actual>

Descripción

Una cadena que contiene la versión actual del firmware del producto.

idRacBuildInfo (sólo lectura)

Valores legales

Una cadena de hasta 16 caracteres ASCII.

Predeterminado

La versión actual de la compilación de firmware del iDRAC6.

Descripción

Una cadena que contiene la versión actual de la compilación del producto.

idRacName (sólo lectura)

Valores legales

Una cadena de hasta 15 caracteres ASCII.

Predeterminado

iDRAC

Descripción

Un nombre asignado por el usuario para identificar a este controlador.

idRacType (sólo lectura)

Valores legales

Identificación del producto

Predeterminado

10

Descripción

Identifica el tipo de controlador de acceso remoto como el iDRAC6.

---

cfgLanNetworking

Este grupo contiene parámetros para configurar la tarjeta de interfaz de red del iDRAC6

Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca la tarjeta de interfaz de red del iDRAC6, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP de la tarjeta de interfaz de red del iDRAC6 cerrarán todas las sesiones de usuario activas y requerirán que los usuarios se vuelvan a conectar con la configuración actualizada de la dirección IP.

cfgNicIPv4Enable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la pila de IPv4 del iDRAC6

cfgNicSelection (lectura/escritura)

Valores legales

0 = Compartido

1 = Compartido con LOM2 de protección contra fallas

2 = Dedicado

3= Compartido con todos los LOM2 de protección contra fallas (sólo iDRAC6 Enterprise)

Predeterminado

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

Descripción

Especifica el modo actual de operación de la tarjeta de interfaz de red (NIC) del RAC. La Tabla B-1 describe los modos admitidos.

Tabla B-1. Modos admitidos de cfgNicSelection

Modo	Descripción
Compartido	Se utiliza cuando la tarjeta integrada de interfaz de red del servidor host se comparte con el RAC en el servidor host. Este modo habilita las configuraciones para utilizar la misma dirección IP en el servidor host y el RAC para tener accesibilidad común en la red.
Compartido con LOM2 de protección contra fallas	Activa la capacidad para formar un equipo entre los controladores integrados de red LOM2 del servidor host.
Dedicado	Especifica que la tarjeta de interfaz de red del RAC se utilice como tarjeta dedicada para accesibilidad remota.
Compartido con todos los LOM2 de protección contra fallas	Activa la capacidad para formar un equipo entre los controladores integrados de red del servidor host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos por medio de la NIC 1 y la NIC 2, pero transmite datos sólo mediante la NIC 1. La protección contra fallas se produce entre la NIC 2 a la NIC 3 y luego a la NIC 4. Si la NIC 4 falla, el dispositivo de acceso remoto vuelve a usar la NIC 1 para todas las transmisiones de datos, pero sólo si la falla original en la NIC 1 se ha corregido.

cfgNicVLanEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva las capacidades de VLAN del RAC/BMC.

cfgNicVLanId (lectura/escritura)

Valores legales

1-4094

Predeterminado

1

Descripción

Especifica la identificación de la VLAN para la configuración de red de la VLAN. Esta propiedad sólo es válida si **cfgNicVLanEnable** se establece como **1** (activada).

cfgNicVLanPriority (lectura/escritura)

Valores legales

De 0 a 7

Predeterminado

0

Descripción

Especifica la prioridad de la VLAN para la configuración de red de la VLAN. Esta propiedad sólo es válida si **cfgNicVLanEnable** se establece como **1** (activada).

cfgDNSDomainNameFromDHCP (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica que el nombre del dominio DNS del iDRAC6 se debe asignar desde el servidor DHCP de la red.

cfgDNSDomainName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII. Al menos uno de los caracteres debe ser alfabético. Los caracteres permitidos son los alfanuméricos, '-'y '.'.

NOTA: Microsoft® Active Directory® sólo admite los nombres de dominio completos (FQDN) de 64 bytes o menos.

Predeterminado

<vacío>

Descripción

Este es el nombre de dominio DNS.

cfgDNSRacName (lectura/escritura)

Valores legales

Una cadena de hasta 63 caracteres ASCII. Al menos un carácter debe ser alfabético.

NOTA: Algunos de los servidores DNS sólo registran nombres de 31 caracteres o menos.

Predeterminado

idrac-<etiqueta de servicio>

Descripción

Muestra el nombre del iDRAC6, el cual es rac-*etiqueta de servicio* de manera predeterminada. Este parámetro sólo es válido si **cfgDNSRegisterRac** se establece como 1 (VERDADERO).

cfgDNSRegisterRac (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Registra el nombre del iDRAC6 en el servidor DNS.

cfgDNSServersFromDHCP (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica si las direcciones IPv4 del servidor DNS se deben asignar a partir del servidor DHCP en la red.

cfgDNSServer1 (lectura/escritura)

Valores legales

Cadena que representa una dirección IPv4 válida. Por ejemplo: 192.168.0.20.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IPv4 del servidor DNS 1

cfgDNSServer2 (lectura/escritura)

Valores legales

Cadena que representa una dirección IPv4 válida. Por ejemplo: 192.168.0.20.

Predeterminado

0.0.0.0

Descripción

Recupera la dirección IPv4 para el servidor DNS 2

cfgNicEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva el controlador de interfaz de red del iDRAC6. Si la NIC está desactivada, las interfaces de red remotas al iDRAC6 ya no serán accesibles.

cfgNicIpAddress (lectura/escritura)

NOTA: Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSO).

Valores legales

Cadena que representa una dirección IPv4 válida. Por ejemplo: 192.168.0.20.

Predeterminado

192.168.0.120

Descripción

Especifica la dirección IPv4 asignada al iDRAC6

cfgNicNetmask (lectura/escritura)

NOTA: Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSO).

Valores legales

Una cadena que representa una máscara de subred válida. Por ejemplo: 255.255.255.0.

Predeterminado

255.255.255.0

Descripción

La máscara de subred utilizada para la dirección IP del iDRAC6.

cfgNicGateway (lectura/escritura)

NOTA: Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSO).

Valores legales

Una cadena que representa una dirección IPv4 de puerta de enlace válida. Por ejemplo: 192.168.0.1.

Predeterminado

192.168.0.1

Descripción

Dirección IPv4 de puerta de enlace del iDRAC6.

cfgNicUseDhcp (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica si se utiliza DHCP para asignar la dirección IP del iDRAC6. Si esta propiedad se establece en 1 (VERDADERO), entonces la dirección IPv4 del iDRAC6, la máscara de subred y la puerta de enlace se asignan a partir del servidor DHCP en la red. Si esta propiedad se establece en **0** (FALSO), el usuario puede configurar las propiedades de **cfgNicIpAddress**, **cfgNicNetmask** y **cfgNicGateway**.

cfgNicMacAddress (sólo lectura)

Valores legales

Cadena que representa la dirección MAC de la NIC del iDRAC6.

Predeterminado

La dirección MAC actual de la NIC del iDRAC6. Por ejemplo, 00:12:67:52:51:A3.

Descripción

La dirección MAC de la NIC del iDRAC6.

---

cfgRemoteHosts

Este grupo contiene propiedades que permiten la configuración del servidor SMTP para las alertas de correo electrónico.

cfgRhostsFwUpdateTftpEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la actualización del firmware del iDRAC6 a partir de un servidor TFTP de red.

cfgRhostsFwUpdateIpAddr (lectura/escritura)

Valores legales

Una cadena que representa una dirección IPv4 válida. Por ejemplo: `192.168.0.61`.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IPv4 del servidor TFTP de red que se utiliza para operaciones de actualización de firmware del iDRAC6 por TFTP

cfgRhostsFwUpdatePath (lectura/escritura)

Valores legales

Una cadena con una longitud máxima de 255 caracteres ASCII

Predeterminado

<vacío>

Descripción

Especifica la ruta de acceso de TFTP en la que se encuentra la imagen de firmware del iDRAC6 en el servidor TFTP. La ruta de acceso de TFTP es relativa a la ruta de acceso raíz de TFTP en el servidor TFTP.

NOTA: Es posible que el servidor aún requiera que se especifique la unidad de disco (por ejemplo, **C:**).

cfgRhostsSmtpServerIpAddr (lectura/escritura)

Valores legales

Una cadena que representa una dirección IPv4 válida de servidor SMTP. Por ejemplo: 192.168.0.55.

Predeterminado

0.0.0.0

Descripción

La dirección IPv4 del servidor SMTP o el servidor TFTP. El servidor SMTP transmite las alertas de correo electrónico desde el iDRAC6 si las alertas están configuradas y activadas. El servidor TFTP transfiere archivos desde y hasta el iDRAC6.

---

cfgUserAdmin

Este grupo ofrece información de configuración de los usuarios que tienen acceso al iDRAC6 por medio de las interfaces remotas disponibles.

Se permiten hasta 16 casos del grupo de usuario. Cada caso representa la configuración de un usuario individual.

cfgUserAdminIndex (sólo lectura)

Valores legales

1 – 16

Predeterminado

<instancia>

Descripción

Este número representa la instancia del usuario.

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

cfgUserAdminPrivilege (lectura/escritura)

Valores legales

0x00000000 a 0x000001ff y 0x0

Predeterminado

0x00000000

Descripción

Esta propiedad especifica los privilegios de autoridad basada en funciones que se otorgan al usuario. El valor se representa como máscara de bits que permite definir cualquier combinación de valores de privilegios. La Tabla B-2 describe los valores de bit de privilegio del usuario que se pueden combinar para crear máscaras de bit.

Tabla B-2. Máscaras de bit para privilegios del usuario

Privilegio del usuario	Máscara de bits de privilegios
Iniciar sesión en el iDRAC	0x0000001
Configurar el iDRAC	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Ejemplos

La Tabla B-3 contiene ejemplos de las máscaras de bits de privilegios para usuarios con uno o más privilegios.

Tabla B-3. Máscaras de bits para privilegios del usuario

Privilegios del usuario	Máscara de bits de privilegios
El usuario no tiene permiso para acceder al iDRAC.	0x00000000
El usuario sólo tiene permitido iniciar sesión en el iDRAC y ver la información de configuración del iDRAC y el servidor.	0x00000001
El usuario puede iniciar sesión en el iDRAC y cambiar la configuración.	0x00000001 + 0x00000002 = 0x00000003
El usuario puede iniciar sesión en el iDRAC, acceder a los medios virtuales y acceder a la redirección de consola.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lectura/escritura)

NOTA: Este valor de propiedad debe ser único entre los nombres de usuario.

Valores legales

Una cadena de hasta 16 caracteres ASCII.

Predeterminado

root (Usuario 2)

<vacío> (Todos los usuarios)

Descripción

El nombre del usuario para este índice. El índice de usuario se crea al escribir una cadena en el campo de este nombre si el índice está vacío. Al escribir una cadena de comillas dobles ("") se elimina al usuario de ese índice. La cadena no debe tener / (barras), \ (barras invertidas), . (puntos), @ (arrobas) ni comillas.

NOTA: Este valor de propiedad debe ser único entre los nombres de usuario.

cfgUserAdminPassword (de sólo escritura)

Valores legales

Una cadena de hasta 20 caracteres ASCII.

Predeterminado

****

Descripción

La contraseña para este usuario. Las contraseñas de usuario están cifradas y no podrán verse ni mostrarse después de que se haya escrito la propiedad.

cfgUserAdminEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1 (Usuario 2)

0 (Todos los otros)

Descripción

Activa o desactiva un usuario individual.

cfgUserAdminSolEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el acceso de usuario serie en la LAN (SOL) para el usuario.

cfgUserAdminIpmiSerialPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

---

cfgEmailAlert

Este grupo contiene los parámetros para configurar las capacidades de alerta por correo electrónico del iDRAC6.

Los apartados siguientes describen los objetos en este grupo. Se permiten hasta cuatro instancias de este grupo.

cfgEmailAlertIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

<instancia>

Descripción

El índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la instancia de alerta.

cfgEmailAlertAddress (lectura/escritura)

Valores legales

Formato de dirección de correo electrónico, con un número máximo de 64 caracteres ASCII.

Predeterminado

<vacío>

Descripción

Especifica el correo electrónico de destino para alertas por correo electrónico, por ejemplo, user1@company.com

cfgEmailAlertCustomMsg (lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Especifica un mensaje personalizado que forma el tema de la alerta.

---

cfgSessionManagement

Este grupo contiene parámetros para configurar la cantidad de sesiones que se pueden conectar al iDRAC6.

Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgSsnMgtRacadmTimeout (lectura/escritura)

Valores legales

De 10 a 1920

Predeterminado

60

Descripción

Define los segundos de expiración de tiempo disponibles para la interfaz de RACADM remota. Si una sesión de RACADM remota permanece inactiva durante más tiempo del especificado, la sesión se cerrará.

cfgSsnMgtConsRedirMaxSessions (lectura / escritura)

Valores legales

De 1 a 4

Predeterminado

2

Descripción

Especifica el número máximo de sesiones de redirección de consola que se permiten en el iDRAC6.

cfgSsnMgtWebserverTimeout (lectura / escritura)

Valores legales

60 – 10800

Predeterminado

1800

Descripción

Define la expiración de tiempo del servidor web. Esta propiedad establece la cantidad de segundos que se permite que la conexión permanezca disponible (sin actividad del usuario). La sesión se cancelará si se alcanza el límite de tiempo que establece esta propiedad. Los cambios de este valor no afectan la sesión actual; usted debe cerrar sesión y reiniciar sesión para que la nueva configuración entre en efecto.

cfgSsnMgtSshIdleTimeout (lectura / escritura)

Valores legales

0 (sin expiración de tiempo)

De 60 a 1920

Predeterminado

300

Descripción

Define la expiración de tiempo de inactividad de Secure Shell. Esta propiedad establece la cantidad de segundos que se permite que la conexión permanezca disponible (sin actividad del usuario). La sesión se cancelará si se alcanza el límite de tiempo que establece esta propiedad. Los cambios de este valor no afectan la sesión actual; usted debe cerrar sesión y reiniciar sesión para que la nueva configuración entre en efecto.

Una sesión de Secure Shell que ha finalizado muestra el siguiente mensaje de error:

```
Connection timed out (Tiempo de espera de conexión finalizado).
```

Después de que el mensaje aparezca, el sistema regresará al shell que generó la sesión de Secure Shell.

cfgSsnMgtTelnetTimeout (lectura/escritura)

Valores legales

0 (sin expiración de tiempo)

De 60 a 1920

Predeterminado

300

Descripción

Define la expiración de tiempo disponible de Telnet. Esta propiedad establece la cantidad de segundos que se permite que la conexión permanezca disponible (sin actividad del usuario). La sesión se cancelará si se alcanza el límite de tiempo que establece esta propiedad. Los cambios de este valor no afectarán la sesión actual (debe cerrar sesión e iniciar sesión nuevamente para que la nueva configuración surta efecto).

Una sesión Telnet finalizada muestra el siguiente mensaje de error:

```
Connection timed out (Tiempo de espera de conexión finalizado).
```

Después de que el mensaje aparezca, el sistema regresará al shell que generó la sesión Telnet.

---

cfgSerial

Este grupo contiene parámetros de configuración de los servicios del iDRAC6.

Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgSerialBaudRate (lectura/escritura)

Valores legales

9600, 28800, 57600, 115200

Predeterminado

57600

Descripción

Establece la velocidad en baudios en el puerto serie del iDRAC6.

cfgSerialConsoleEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de la consola serie del RAC.

cfgSerialConsoleQuitKey (lectura/escritura)

Valores legales

Una cadena de hasta 4 caracteres.

Predeterminado

^\ (<Ctrl><\>)

NOTA: El carácter "^" es la tecla <Ctrl>.

Descripción

Esta tecla o combinación de teclas finaliza la redirección de consola de texto cuando se utiliza el comando **connect com2**. El valor de **cfgSerialConsoleQuitKey** se puede representar de alguna de las siguientes maneras:

- Valor decimal: por ejemplo, "95"
- Valor hexadecimal: por ejemplo, "0x12"
- Valor octal: por ejemplo, "007"
- Valor ASCII: por ejemplo, "^a"

Los valores ASCII se pueden representar con los siguientes códigos de escape de teclas:

(a) ^ seguido de cualquier letra (a-z, A-Z)

(b) ^ seguido de los caracteres especiales indicados: [ ] \ ^ _

cfgSerialConsoleIdleTimeout (lectura/escritura)

Valores legales

0 = Sin expiración de tiempo

De 60 a 1920

Predeterminado

300

Descripción

La cantidad máxima de segundos a esperar antes de desconectar una sesión serie sin actividad.

cfgSerialConsoleNoAuth (lectura/escritura)

Valores legales

0 (activa la autenticación de inicio de sesión serie)

1 (desactiva la autenticación de inicio de sesión serie)

Predeterminado

0

Descripción

Activa o desactiva la autenticación del inicio de sesión de la consola serie del RAC.

cfgSerialConsoleCommand (lectura/escritura)

Valores legales

Una cadena de hasta 128 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el comando serie que se ejecutará después de que un usuario inicie sesión en la interfaz de consola serie.

cfgSerialHistorySize (lectura/escritura)

Valores legales

De 0 a 8192

Predeterminado

8192

Descripción

Especifica el tamaño máximo del búfer de historial de la conexión serie.

cfgSerialCom2RedirEnable (lectura/escritura)

Predeterminado

1

Valores legales

1 (VERDADERO)

0 (FALSO)

Descripción

Activa o desactiva la consola para la redirección del puerto COM 2.

cfgSerialSshEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de Secure Shell (SSH) en el iDRAC6.

cfgSerialTelnetEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de la consola Telnet en el iDRAC6.

---

cfgOobSnmp

El grupo contiene parámetros para configurar las capacidades de excepción y de agente SNMP del iDRAC6.

Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgOobSnmpAgentCommunity (lectura/escritura)

Valores legales

Una cadena de hasta 31 caracteres.

Predeterminado

público

Descripción

Especifica el nombre de comunidad SNMP que se utiliza para las excepciones SNMP.

cfgOobSnmpAgentEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el agente SNMP en el iDRAC6.

---

cfgRacTuning

Este grupo se usa para configurar varias propiedades de configuración del iDRAC6, por ejemplo, las restricciones de puertos de seguridad y los puertos válidos.

cfgRacTuneConRedirPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

5900

Descripción

Especifica el puerto a utilizarse para el teclado, ratón, video y trafico de medios virtuales al RAC.

cfgRacTuneRemoteRacadmEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de RACADM remoto en el iDRAC.

cfgRacTuneCtrlEConfigDisable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la capacidad de desactivar la facultad del usuario local para configurar el iDRAC a partir de la ROM de opción de la POST (Power-On Self-Test [autoprueba de encendido]) del BIOS.

cfgRacTuneHttpPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

80

Descripción

Especifica el número de puerto que se debe usar para la comunicación de red HTTP con el iDRAC6.

cfgRacTuneHttpsPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

443

Descripción

Especifica el número de puerto que se debe usar para la comunicación de red HTTPS con el iDRAC6.

cfgRacTuneIpRangeEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de validación de rango de dirección IPv4 del iDRAC6.

cfgRacTuneIpRangeAddr (lectura/escritura)

Valores legales

Una cadena con formato de dirección IPv4, por ejemplo, 192.168.0.44

Predeterminado

192.168.1.1

Descripción

Especifica el patrón de bits de dirección IPv4 aceptable en posiciones determinadas por los números 1 en la propiedad de máscara de rango (**cfgRacTuneIpRangeMask**)

cfgRacTuneIpRangeMask (lectura/escritura)

Valores legales

Una cadena con formato de dirección IPv4, por ejemplo, 255.255.255.0

Predeterminado

255.255.255.0

Descripción

Valores de máscara de IP estándares con bits justificados a la izquierda Por ejemplo: 255.255.255.0.

cfgRacTuneIpBlkEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de bloqueo de direcciones IPv4 del iDRAC6.

cfgRacTuneIpBlkFailCount (lectura/escritura)

Valores legales

De 2 a 16

Predeterminado

5

Descripción

El número máximo de fallas de inicio de sesión que se permite en la ventana (**cfgRacTuneIpBlkFailWindow**) antes de rechazar los intentos de inicio de sesión de la dirección IP.

cfgRacTuneIpBlkFailWindow (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

60

Descripción

Define el período en segundos durante el cual se contarán los intentos fallidos. Cuando los intentos fallidos superan este límite, se borran de la cuenta.

cfgRacTuneIpBlkPenaltyTime (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

300

Descripción

Define el período en segundos durante el que se rechazarán las solicitudes de inicio de sesión provenientes de una dirección IP con fallas excesivas.

cfgRacTuneSshPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

22

Descripción

Especifica el número de puerto que se usa para la interfaz SSH del iDRAC6.

cfgRacTuneTelnetPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

23

Descripción

Especifica el número de puerto que se usa para la interfaz Telnet del iDRAC6.

cfgRacTuneConRedirEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa la redirección de consola.

cfgRacTuneConRedirEncryptEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Cifra el vídeo en una sesión de redirección de consola.

cfgRacTuneAsrEnable (lectura / escritura)

NOTA: Este objeto requiere de un restablecimiento del iDRAC6 antes de activarse.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de captura de pantalla de último bloqueo del iDRAC6.

cfgRacTuneDaylightOffset (lectura / escritura)

Valores legales

De 0 a 60

Predeterminado

0

Descripción

Especifica la compensación de horario de verano (en minutos) que se utiliza para la hora del RAC.

cfgRacTuneTimezoneOffset (lectura / escritura)

Valores legales

–720 – 780

Predeterminado

0

Descripción

Especifica la diferencia de zona horaria (en minutos) en relación con GMT/UTC que se utiliza para la hora del RAC. A continuación se enumeran algunas diferencias de zona horaria para los Estados Unidos:

-480 (PST: hora estándar de la costa del Pacífico)

-420 (MST: hora estándar de la zona de las montañas)

-360 (CST: hora estándar central)

-300 (EST: hora estándar de la costa Este)

cfgRacTuneLocalServerVideo (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa (enciende) o desactiva (apaga) el vídeo del servidor local.

cfgRacTuneLocalConfigDisable (lectura/escritura)

Valores legales

0 (VERDADERO)

1 (FALSO)

Predeterminado

0

Descripción

Al establecerlo en 1, desactiva el acceso de escritura a los datos de configuración del iDRAC6.

cfgRacTuneWebserverEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva el servidor web del iDRAC6. Si esta propiedad está desactivada, no se podrá tener acceso al iDRAC6 por medio de exploradores web clientes. Esta propiedad no tiene ningún efecto en las interfaces Telnet, SSH o RACADM.

---

ifcRacManagedNodeOs

Este grupo contiene propiedades que describen el sistema operativo del servidor administrado.

Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

ifcRacMnOsHostname (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

<vacío>

Descripción

El nombre de host del servidor administrado.

ifcRacMnOsOsName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

<vacío>

Descripción

El nombre del sistema operativo del servidor administrado.

---

cfgRacSecurity

Este grupo se usa para configurar los valores relacionados con la función de solicitud de firma de certificado (CSR) SSL del iDRAC6. Las propiedades en este grupo se deben configurar antes de generar una CSR desde el iDRAC6.

Consulte los detalles del subcomando **sslcsrgen** de RACADM para obtener más información sobre cómo generar solicitudes de firma de certificado.

cfgRacSecCsrCommonName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el nombre común (CN) de una CRS que debe ser un IP o el nombre del iDRAC como se expresa en el certificado.

cfgRacSecCsrOrganizationName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el nombre de la organización (O) de la CSR.

cfgRacSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la unidad organizacional (OU) de la CSR.

cfgRacSecCsrLocalityName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la localidad (L) de la CSR.

cfgRacSecCsrStateName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el nombre del estado (S) de la CSR.

cfgRacSecCsrCountryCode (lectura/escritura)

Valores legales

Una cadena de hasta 2 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el código de país (CC) de la CSR.

cfgRacSecCsrEmailAddr (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la dirección de correo electrónico de la CSR.

cfgRacSecCsrKeySize (lectura/escritura)

Valores legales

1024

2048

4096

Predeterminado

1024

Descripción

Especifica el tamaño de la clave asimétrica de SSL para la CSR.

---

cfgRacVirtual

Este grupo contiene parámetros para configurar la función de medios virtuales del iDRAC6. Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgVirMediaAttached (lectura / escritura)

Valores legales

0 = Desconectar

1 = Conectar

2 = Conectar automáticamente

Predeterminado

0

Descripción

Este objeto se usa para conectar dispositivos virtuales al sistema por medio del bus USB. Cuando los dispositivos se conecten, el servidor reconocerá los dispositivos USB de almacenamiento masivo que estén conectados al sistema. Esto equivale a conectar una unidad USB de CD-ROM/disquete local a un puerto USB del sistema. Cuando los dispositivos estén conectados usted podrá conectar los dispositivos virtuales de manera remota utilizando la interfaz web del iDRAC6 o la interfaz de línea de comandos. Si asigna el valor de **0** a este objeto, hará que los dispositivos se desconecten del bus USB.

cfgVirtualBootOnce (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de iniciar una vez a partir de los medios virtuales del iDRAC6.

cfgVirMediaFloppyEmulation (lectura / escritura)

NOTA: Los medios virtuales deben volver a conectarse (utilizando cfgVirMediaAttached) para que este cambio tenga efecto.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Cuando se define como 0, los sistemas operativos Windows reconocen la unidad de disquete virtual como unidad de disco extraíble. Los sistemas operativos Windows asignarán una letra de unidad C: o posterior durante la enumeración. Cuando se establezca como 1, los sistemas operativos Windows detectarán la unidad de disquete virtual como unidad de disquete. Los sistemas operativos Windows asignarán una letra de unidad A: o B:.

cfgVirMediaKeyEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de memoria de medios virtuales del RAC.

---

cfgActiveDirectory

Este grupo contiene parámetros para configurar la característica Active Directory del iDRAC6.

cfgADRacDomain (lectura/escritura)

Valores legales

Cualquier cadena de texto imprimible de hasta 254 caracteres, sin espacio en blanco.

Predeterminado

<vacío>

Descripción

El dominio de Active Directory donde reside el iDRAC6.

cfgADRacName (lectura/escritura)

Valores legales

Cualquier cadena de texto imprimible hasta 254 caracteres, sin espacio en blanco.

Predeterminado

<vacío>

Descripción

El nombre del iDRAC6 según está registrado en el bosque de Active Directory.

cfgADEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la autenticación de usuario de Active Directory en el iDRAC6. Si esta propiedad está desactivada, se usará sólo la autenticación local del iDRAC6 para los inicios de sesión de usuarios.

cfgADSSOEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la autenticación de inicio de sesión único de Active Directory en el iDRAC6.

cfgADSmartCardLogonEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el inicio de sesión con tarjeta inteligente en el iDRAC6.

cfgADCRLEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la revisión de la lista de revocación de certificados (CRL) para los usuarios de tarjeta inteligente basados en Active Directory.

cfgADDomainController1 (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor LDAP.

cfgADDomainController2 (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor LDAP.

cfgADDomainController3 (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor LDAP.

cfgADAuthTimeout (lectura / escritura)

Valores legales

15 – 300 segundos.

Predeterminado

120

Descripción

Especifica el número de segundos que se debe esperar para que las solicitudes de autenticación de Active Directory finalicen antes de agotar el tiempo de espera.

cfgADType (lectura / escritura)

Valores legales

1 (esquema ampliado)

2 (esquema estándar)

Predeterminado

1

Descripción

Determina el tipo de esquema que se utiliza con Active Directory.

cfgADGlobalCatalog1 (lectura / escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADGlobalCatalog2 (lectura / escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADGlobalCatalog3 (lectura / escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII que representan una dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

<vacío>

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADCertValidationEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la validación de certificados de Active Directory como parte del proceso de configuración de Active Directory.

---

cfgStandardSchema

Este grupo contiene parámetros para establecer la configuración del esquema estándar de Active Directory.

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

Un número entero entre 1 y 5.

Predeterminado

<instancia>

Descripción

Índice del grupo de funciones como está registrado en Active Directory

cfgSSADRoleGroupName (lectura/escritura)

Valores legales

Cualquier cadena de texto que se pueda imprimir con 254 caracteres como máximo.

Predeterminado

<vacío>

Descripción

Nombre del grupo de funciones como está registrado en el bosque de Active Directory

cfgSSADRoleGroupDomain (lectura/escritura)

Valores legales

Cualquier cadena de texto imprimible hasta 254 caracteres, sin espacio en blanco.

Predeterminado

<vacío>

Descripción

El dominio de Active Directory donde reside el grupo de funciones.

cfgSSADRoleGroupPrivilege (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

<vacío>

Descripción

Utilice los números de máscara de bits que aparecen en la Tabla B-4 para establecer los privilegios de autoridad en base a una función para un grupo de funciones.

Tabla B-4. Máscaras de bits para los privilegios del grupo de funciones

Privilegio del grupo de funciones	Máscara de bits
Iniciar sesión en el iDRAC	0x00000001
Configurar el iDRAC	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a redirección de consola	0x00000020
Acceder a los medios virtuales	0x00000040
Probar alertas	0x00000080
Ejecutar comandos de depuración	0x00000100

---

cfgIpmiSol

Este grupo se usa para configurar las capacidades de comunicación en serie en la LAN (SOL) del sistema.

cfgIpmiSolEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva SOL.

cfgIpmiSolBaudRate (lectura/escritura)

Valores legales

9600, 19200, 57600, 115200

Predeterminado

115200

Descripción

La velocidad en baudios de la comunicación en serie en la LAN.

cfgIpmiSolMinPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

Especifica el nivel de privilegio mínimo que se requiere para el acceso de comunicación en serie en la LAN.

cfgIpmiSolAccumulateInterval (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

10

Descripción

Especifica la cantidad típica de tiempo que el iDRAC6 espera antes de transmitir un paquete parcial de datos de caracteres de comunicación en serie en la LAN. Este valor consta de incrementos de 5 ms basados en unos.

cfgIpmiSolSendThreshold (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

255

Descripción

El valor del límite de umbral de SOL. Especifica el número máximo de bytes que se van a almacenar en búfer antes de enviar a un paquete de datos de comunicación serie en la LAN.

---

cfgIpmiLan

Este grupo se usa para configurar las capacidades de IPMI en la LAN del sistema.

cfgIpmiLanEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de IPMI en la LAN.

cfgIpmiLanPrivilegeLimit (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

Especifica el nivel de privilegio máximo que se permite para el acceso de IPMI en la LAN

cfgIpmiLanAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva las alertas globales por correo electrónico. Esta propiedad anula todas las propiedades individuales de activación o desactivación de alertas por correo electrónico.

cfgIpmiEncryptionKey (lectura/escritura)

Valores legales

Una cadena de dígitos hexadecimales de 0 a 40 caracteres sin espacios Solo se permite una cantidad igual de dígitos.

Predeterminado

00000000000000000000

Descripción

La clave de cifrado de IPMI.

cfgIpmiPetCommunityName (lectura/escritura)

Valores legales

Una cadena de hasta 18 caracteres.

Predeterminado

público

Descripción

El nombre de comunidad SNMP para las excepciones.

---

cfgIpmiPetIpv6

Este grupo se usa para configurar las excepciones de sucesos de plataforma IPv6 en el servidor administrado.

cfgIpmiPetIPv6Index (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

<Valor de índice>

Descripción

Identificador único para el índice que corresponde a la excepción.

cfgIpmiPetIPv6AlertDestIpAddr

Valores legales

Dirección IPv6

Predeterminado

<vacío>

Descripción

Configura la dirección IP de destino de alerta de IPv6 para la excepción.

cfgIpmiPetIPv6AlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el destino de alerta IPv6 para la captura.

---

cfgIpmiPef

Este grupo se utiliza para configurar los filtros de eventos de plataforma que están disponibles en el servidor administrado.

Los filtros de eventos se pueden utilizar para controlar las acciones relacionadas con políticas que se desencadenan cuando ocurren sucesos críticos en el servidor administrado.

cfgIpmiPefName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

El nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de eventos de plataforma.

cfgIpmiPefIndex (lectura/escritura)

Valores legales

1 – 19

Predeterminado

El valor de índice de un objeto de filtro de eventos de plataforma.

Descripción

Especifica el índice de un filtro de eventos de plataforma específico.

cfgIpmiPefAction (lectura/escritura)

Valores legales

0 (ninguno)

1 (apagar)

2 (restablecer)

3 (realizar ciclo de encendido)

Predeterminado

0

Descripción

Especifica la acción que se realiza en el servidor administrado al momento en que se activa la alerta.

cfgIpmiPefEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva un filtro de eventos de plataforma específica.

---

cfgIpmiPet

Este grupo se usa para configurar las excepciones de eventos de plataforma en el servidor administrado.

cfgIpmiPetIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

El valor índice de una excepción específica de eventos de plataforma.

Descripción

Identificador único para el índice que corresponde a la excepción.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

Valores legales

Una cadena que representa una dirección IPv4 válida. Por ejemplo: `192.168.0.67`.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP de destino del receptor de excepciones en la red. El receptor de excepciones recibe una excepción SNMP cuando se presenta un evento en el servidor administrado.

cfgIpmiPetAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva una excepción específica.

---

cfgUserDomain

Este grupo se utiliza para configurar los nombres de dominio para los usuarios de Active Directory.. Pueden configurarse hasta un máximo de 40 nombres de dominio por vez.

cfgUserDomainIndex (sólo lectura)

Valores legales

1 – 40

Predeterminado

Valor del índice

Descripción

Representa un dominio específico

cfgUserDomainName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres ASCII.

Predeterminado

<vacío>

Descripción

Especifica el nombre de dominio de usuario de Active Directory

---

cfgServerPower

Este grupo proporciona varias funciones de administración de energía.

cfgServerPowerStatus (sólo lectura)

Valores legales

1 (ENCENDIDO)

0 (APAGADO)

Predeterminado

<estado de alimentación del servidor actual>

Descripción

Representa el estado de la alimentación del servidor, ya sea ENCENDIDO o APAGADO

cfgServerPowerAllocation (sólo lectura)

NOTA: Si hay más de un suministro de energía, esta propiedad hace referencia al suministro de energía de capacidad mínima.

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa el suministro de energía disponible para el uso del servidor

cfgServerActualPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa el consumo de alimentación del servidor actual

cfgServerMinPowerCapacity (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa la capacidad mínima de alimentación del servidor.

cfgServerMaxPowerCapacity (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa la capacidad máxima de alimentación del servidor.

cfgServerPeakPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<consumo de energía máximo del servidor>

Descripción

Representa el consumo máximo de energía del servidor hasta el momento

cfgServerPeakPowerConsumptionTimestamp (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Fecha y hora del consumo máximo de energía

Descripción

Hora en que se registró el consumo máximo de energía

cfgServerPowerConsumptionClear (sólo escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

****

Descripción

Restablece la propiedad **cfgServerPeakPowerConsumption (lectura/escritura)** a 0 y la propiedad **cfgServerPeakPowerConsumptionTimestamp** a la hora actual del iDRAC

cfgServerPowerCapWatts (lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servidor en vatios

Descripción

Representa el umbral de alimentación del servidor en vatios.

cfgServerPowerCapBtuhr (lectura / escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servidor en BTU/h

Descripción

Representa el umbral de alimentación del servidor expresado en BTU/h

cfgServerPowerCapPercent (lectura / escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servidor en porcentaje.

Descripción

Representa el umbral de alimentación del servidor expresado en porcentajes

---

cfgIPv6LanNetworking

Este grupo se utiliza para configurar IPv6 sobre las capacidades de sistema de red de LAN

cfgIPv6Enable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la pila de IPv6 del iDRAC6

cfgIPv6Address1 (lectura / escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del iDRAC6

cfgIPv6Gateway (lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 de puerta de enlace del iDRAC6.

cfgIPv6PrefixLength (lectura/escritura)

Valores legales

1-128

Predeterminado

64

Descripción

Longitud del prefijo para dirección IPv6 del iDRAC6.

cfgIPv6AutoConfig (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la opción Auto Config de IPv6.

cfgIPv6LinkLocalAddress (sólo lectura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección local del vínculo IPv6 del iDRAC6.

cfgIPv6Address2 (sólo lectura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del iDRAC6

cfgIPv6DNSServersFromDHCP6 (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica si cfgIPv6DNSServer1 y cfgIPv6DNSServer2 son direcciones IPv6 de DHCP o estáticas.

cfgIPv6DNSServer1 (lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del servidor DNS

cfgIPv6DNSServer2 (lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del servidor DNS

---

cfgIPv6URL

Este grupo especifica las propiedades utilizadas para configurar la dirección URL de IPv6 del iDRAC6.

cfgIPv6URLstring (sólo lectura)

Valores legales

Una cadena de hasta 80 caracteres

Predeterminado

<vacío>

Descripción

La dirección URL de IPv6 del iDRAC6.

---

cfgIpmiSerial

Este grupo especifica las propiedades que se utilizan para configurar la interfaz serie de IPMI del BMC.

cfgIpmiSerialConnectionMode (lectura/escritura)

Valores legales

0 (terminal)

1 (básico)

Predeterminado

1

Descripción

Cuando la propiedad **cfgSerialConsoleEnable** del iDRAC6 se establece como 0 (desactivada), el puerto serie del iDRAC6 se convierte en el puerto serie de IPMI. Esta propiedad determina el modo definido por IPMI del puerto serie.

En el modo básico, el puerto utiliza datos binarios con la finalidad de comunicarse con un programa de aplicación en el cliente serie. En el modo terminal, el puerto supone que hay un terminal ASCII sin capacidad de procesamiento conectado y permite que se introduzcan comandos muy simples.

cfgIpmiSerialBaudRate (lectura/escritura)

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

Especifica la velocidad en baudios de la conexión serie en la IPMI.

cfgIpmiSerialChanPrivLimit (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

Especifica el nivel de privilegio máximo que se permite en el canal serie de IPMI.

cfgIpmiSerialFlowControl (lectura/escritura)

Valores legales

0 (ninguno)

1 (CTS/RTS)

2 (XON/XOFF)

Predeterminado

1

Descripción

Especifica la configuración del control de flujo para el puerto serie de IPMI.

cfgIpmiSerialHandshakeControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva el control de protocolo de enlace del modo de terminal de IPMI.

cfgIpmiSerialLineEdit (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva la edición de línea en la interfaz serie de IPMI.

cfgIpmiSerialEchoControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva el control de eco en la interfaz serie de IPMI.

cfgIpmiSerialDeleteControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

Activa o desactiva el control de eliminación en la interfaz serie de IPMI.

cfgIpmiSerialNewLineSequence (lectura/escritura)

Valores legales

0 (ninguno)

1 (CR-LF)

2 (NULO)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Predeterminado

1

Descripción

Determina la especificación de secuencia de nueva línea para la interfaz serie de IPMI.

cfgIpmiSerialInputNewLineSequence (lectura/escritura)

Valores legales

0 (<ENTRAR>)

1 (NULO)

Predeterminado

1

Descripción

Determina la especificación de secuencia de nueva línea de entrada para la interfaz serie de IPMI.

---

cfgSmartCard

Este grupo especifica las propiedades utilizadas para respaldar el acceso al iDRAC6 mediante una tarjeta inteligente.

cfgSmartCardLogonEnable (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

2 (Activado con RACADM remota)

Predeterminado

0

Descripción

Activa, desactiva o activa con respaldo de RACADM remota para acceso al iDRAC6 con una tarjeta inteligente.

cfgSmartCardCRLEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la lista de revocación de certificados (CRL)

---

cfgNetTuning

Este grupo permite que los usuarios configuren los parámetros avanzados de la interfaz de red de la tarjeta de interfaz de red del RAC. Cuando se configuran, los valores actualizados pueden tardar hasta un minuto en activarse.

PRECAUCIÓN: Tenga precaución extrema cuando modifique las propiedades en este grupo. La modificación incorrecta de las propiedades en este grupo puede provocar que la tarjeta de interfaz de red del RAC no funcione.

cfgNetTuningNicAutoneg (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa la negociación automática del dúplex y la velocidad del vínculo físico. Si está activada, la negociación automática tiene prioridad sobre los valores establecidos en los objetos **cfgNetTuningNic100MB** y **cfgNetTuningNicFullDuplex**.

cfgNetTuningNic100MB (lectura/escritura)

Valores legales

0 (10 Mb)

1 (100 Mb)

Predeterminado

1

Descripción

Especifica la velocidad que se utiliza para la tarjeta de interfaz de red del RAC. Esta propiedad no se utilizará si el objeto **cfgNetTuningNicAutoNeg** se establece como **1** (activado).

cfgNetTuningNicFullDuplex (lectura/escritura)

Valores legales

0 (Semidúplex)

1 (Dúplex completo)

Predeterminado

1

Descripción

Especifica la configuración de dúplex de la tarjeta de interfaz de red del RAC. Esta propiedad no se utilizará si el objeto **cfgNetTuningNicAutoNeg** se establece como **1** (activado).

cfgNetTuningNicMtu (lectura/escritura)

Valores legales

De 576 a 1500

Predeterminado

1500

Descripción

El tamaño en bytes de la unidad de transmisión máxima usada por la NIC del iDRAC6.

Regresar a la página de contenido

Regresar a la página de contenido

Interfaces admitidas de RACADM

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

La Tabla C-1 a continuación contiene una descripción general de los subcomandos de RACADM y la compatibilidad correspondiente de los mismos con interfaces.

Tabla C-1. Compatibilidad de interfaces de los subcomandos de RACADM

Subcomando	Telnet/SSH/serie	RACADM local	RACADM remota
arp	✔	✘	✔
clearasrscreen	✔	✔	✔
clrraclog	✔	✔	✔
clrsel	✔	✔	✔
coredump	✔	✘	✔
coredumpdelete	✔	✔	✔
fwupdate	✔	✔	✔
getconfig	✔	✔	✔
getniccfg	✔	✔	✔
getraclog	✔	✔	✔
getractime	✔	✔	✔
getsel	✔	✔	✔
getssninfo	✔	✔	✔
getsvctag	✔	✔	✔
getsysinfo	✔	✔	✔
gettracelog	✔	✔	✔
help	✔	✔	✔
ifconfig	✔	✘	✔
netstat	✔	✘	✔
ping	✔	✘	✔
racdump	✔	✘	✔
racreset	✔	✔	✔
racresetcfg	✔	✔	✔
serveraction	✔	✔	✔
setniccfg	✔	✔	✔
sslcertdownload	✘	✔	✔
sslcertupload	✘	✔	✔
sslcertview	✔	✔	✔
sslcsrgen	✘	✔	✔
sslkeyupload	✘	✔	✔
testemail	✔	✔	✔
testtrap	✔	✔	✔
vmdisconnect	✔	✔	✔
vmkey	✔	✔	✔
usercertupload	✘	✔	✔
usercertview	✔	✔	✔
localConRedirDisable	✘	✔	✘
✔ = compatible; ✘ = no compatible			

Regresar a la página de contenido

Regresar a la página de contenido

Introducción al iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Integrated Dell™ Remote Access Controller 6 (iDRAC6) es una solución de hardware y software de administración de sistemas que brinda capacidades de administración remota, recuperación de sistemas bloqueados y funciones de control de alimentación para los sistemas Dell PowerEdge™.

El iDRAC6 usa un microprocesador integrado de sistema en chip para el sistema de control y supervisión remoto. El iDRAC6 coexiste en la placa base con el servidor PowerEdge administrado. El sistema operativo del servidor se encarga de la ejecución de aplicaciones; el iDRAC6 se encarga de la supervisión y administración del entorno del servidor y el estado fuera del sistema operativo.

Usted puede configurar el iDRAC6 para que éste le envíe alertas por correo electrónico o de excepción de protocolo simple de administración de red (Simple Network Management Protocol, SNMP) ante advertencias o errores. Para ayudar a diagnosticar la causa probable de un bloqueo de sistema, iDRAC6 puede registrar datos de eventos y capturar una imagen de la pantalla cuando detecta que el sistema se ha bloqueado.

La interfaz de red del iDRAC6 se activa con una dirección IP estática 192.168.0.120 de manera predeterminada. Se debe configurar antes de que se pueda acceder al iDRAC6. Una vez que el iDRAC6 esté configurado en la red, se podrá tener acceso a la dirección IP asignada del mismo por medio de la interfaz web del iDRAC6, Telnet o Secure Shell (SSH) y los protocolos de administración de red admitidos, por ejemplo, la interfaz de administración de plataforma inteligente (IPMI).

Características de administración del iDRAC6 Express

El iDRAC6 Express ofrece las siguientes funciones administrativas:

- Registro de sistema dinámico de nombres de dominio (DDNS)
- Administración remota del sistema y supervisión utilizando una interfaz web y línea de comandos SM-CLP sobre una conexión Telnet o SSH.
- Compatibilidad con la autenticación de Microsoft® Active Directory®: centraliza las identificaciones y contraseñas de usuario del iDRAC6 en Active Directory por medio del esquema estándar o de un esquema ampliado
- Supervisión: brinda acceso a la información del sistema y al estado de los componentes
- Acceso a los registros del sistema: brinda acceso al registro de eventos del sistema, el registro del iDRAC6 y la última pantalla de bloqueo del sistema bloqueado o que no responde que es independiente del estado del sistema operativo
- Integración del software Dell OpenManage™: permite iniciar la interfaz web del iDRAC6 desde Dell OpenManage Server Administrator o Dell OpenManage IT Assistant
- Alerta del iDRAC6: alerta sobre problemas potenciales del nodo administrado por medio de un mensaje de correo electrónico o una excepción SNMP
- Administración de energía remota: brinda funciones de administración de energía remota, como el apagado y restablecimiento, a partir de una consola de administración
- Compatibilidad con la interfaz de administración de plataforma inteligente (IPMI)
- Cifrado de capa de sockets seguros (SSL): ofrece administración remota y segura de sistemas por medio de la interfaz web
- Administración de seguridad a nivel de contraseña: evita el acceso no autorizado a un sistema remoto.
- Autoridad en base a funciones: proporciona permisos asignables para distintas tareas de administración de sistemas
- Compatibilidad con IPv6: agrega funciones IPv6 como la capacidad de acceder a la interfaz web del iDRAC6 mediante una dirección IPv6, especifica la dirección IPv6 para la tarjeta de interfaz de red del iDRAC6 y también especifica un número de destino para configurar un destino de alerta SNMP de IPv6.
- Compatibilidad con WS-MAN: ofrece administración de acceso de red mediante el uso del protocolo de servicios web para administración (WS-MAN).
- Compatibilidad con SM-CLP: agrega compatibilidad con el protocolo de línea de comandos para la administración de servidores (SM-CLP), que proporciona estándares para implementaciones de interfaz de línea de comandos de administración de sistemas.
- Reversión y recuperación de firmware: le permite iniciar (o revertir) desde una imagen de firmware de su elección.

Para obtener más información acerca del iDRAC6 Express, consulte el *Manual del propietario de hardware* en **support.dell.com\manuals**.

---

iDRAC6 Enterprise y tarjeta multimedia vFlash

Agrega compatibilidad con RACADM, KVM virtual, características de medios virtuales, una tarjeta de interfaz de red dedicada y flash virtual (con una tarjeta multimedia opcional vFlash) El uso de flash virtual permite almacenar imágenes de inicio de emergencia y herramientas de diagnóstico en la tarjeta multimedia vFlash. Para obtener más información acerca del iDRAC6 Enterprise y la tarjeta multimedia vFlash, consulte el *Manual del propietario de hardware* en **support.dell.com\manuals**.

La Tabla 1-1 enumera las funciones disponibles para BMC, iDRAC6 Express, iDRAC6 Enterprise y la tarjeta multimedia vFlash.

Tabla 1-1. Lista de funciones del iDRAC6

Componente	BMC	iDRAC6 Express	iDRAC6 Enterprise	Tarjeta multimedia vFlash
Compatibilidad con interfaces y estándares				
IPMI 2.0	✔	✔	✔	✔
Interfaz gráfica web del usuario	✘	✔	✔	✔
SNMP	✘	✔	✔	✔
WSMAN	✘	✔	✔	✔
SMASH-CLP	✘	✔	✔	✔
Línea de comandos RACADM	✘	✘	✔	✔
Conductividad				
Modos de red compartida y de recuperación ante fallas	✔	✔	✔	✔
IPv4	✔	✔	✔	✔
Etiquetado VLAN	✔	✔	✔	✔
IPv6	✘	✔	✔	✔
DNS dinámico	✘	✔	✔	✔
NIC dedicado	✘	✘	✔	✔
Seguridad y autenticación				
Autorizaciones en base a funciones	✔	✔	✔	✔
Usuarios locales	✔	✔	✔	✔
Active Directory	✘	✔	✔	✔
Autenticación de dos factores	✘	✔	✔	✔
Inicio de sesión único	✘	✔	✔	✔
Cifrado SSL	✔	✔	✔	✔
Corrección y administración remota				
Actualización remota de firmware	✔ [1]	✔	✔	✔
Control de alimentación de servidor	✔ [1]	✔	✔	✔
Comunicación en serie en la LAN (con proxy)	✔	✔	✔	✔
Comunicación en serie en la LAN (sin proxy)	✘	✔	✔	✔
Límites de alimentación	✘	✔	✔	✔
Captura de pantalla de último bloqueo	✘	✔	✔	✔
Captura de inicio	✘	✔	✔	✔
Medios virtuales	✘	✘	✔	✔
Consola virtual	✘	✘	✔	✔
Consola virtual compartida	✘	✘	✔	✔
Unidad flash virtual	✘	✘	✘	✔
Supervisión				
Alerta y supervisión de sensor	✔ [1]	✔	✔	✔
Supervisión de alimentación en tiempo real	✘	✔	✔	✔
Gráficos de alimentación en tiempo real	✘	✔	✔	✔
Medidores de datos históricos de alimentación	✘	✔	✔	✔
Registro				
Registro de eventos del sistema (SEL)	✔	✔	✔	✔
Registro del RAC	✘	✔	✔	✔
Registro de rastreo	✘	✔	✔	✔
[1]–Esta función sólo se encuentra disponible a través de IPMI y no a través de una interfaz gráfica web del usuario				
✔ = compatible; ✘ = no compatible				

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Autenticación de usuarios por medio de Active Directory (opcional) o identificaciones y contraseñas de usuarios almacenadas en hardware
- Autoridad en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de identificación y contraseña de usuario por medio de la interfaz web o SM-CLP

- Las interfaces web y SM-CLP, que son compatibles con los cifrados de 128 bits y 40 bits (para países en los que no se aceptan 128 bits), usando el estándar SSL 3.0
- Configuración de expiración de tiempo de la sesión (en segundos) por medio de la interfaz web o SM-CLP
- Puertos IP que se pueden configurar (en los casos correspondientes)

  NOTA: Telnet no admite el cifrado SSL.

- SSH, que usa una capa de transporte cifrado para ofrecer mayor seguridad
- Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando ésta ha superado el límite
- Capacidad para limitar el rango de dirección IP para clientes que se conecten con el iDRAC6
- Autenticación de la tarjeta inteligente

Plataformas admitidas

Para conocer las plataformas compatibles más recientes, consulte el archivo léame del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra disponible en **support.dell.com\manuals** y en el DVD *Dell Systems Management Tools and Documentation* que se suministra con el sistema.

Sistemas operativos admitidos

Para obtener información actualizada, consulte el archivo léame del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra disponible en **support.dell.com\manuals** y en el DVD *Dell Systems Management Tools and Documentation* que se suministra con el sistema.

Exploradores web admitidos

Para obtener información actualizada, consulte el archivo léame del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra disponible en **support.dell.com\manuals** y en el DVD *Dell Systems Management Tools and Documentation* que se suministra con el sistema.

NOTA: A causa de defectos serios de seguridad, se ha interrumpido la compatibilidad con SSL 2.0. Su explorador debe estar configurado para permitir SSL 3.0 para que funcione correctamente.

Conexiones de acceso remoto admitidas

La Tabla 1-2 muestra una lista de las funciones de conexión.

Tabla 1-2. Conexiones de acceso remoto admitidas

Conexión	Características
Tarjeta de interfaz de red del iDRAC6	- 10Mbps/100Mbs/Ethernet - Compatibilidad con DHCP - Notificación de eventos por correo electrónico y excepciones SNMP - Compatibilidad para el shell de comandos de SM-CLP (Telnet o SSH) para operaciones como la configuración del iDRAC6, el inicio del sistema, el restablecimiento, el encendido y los comandos de apagado - Compatibilidad para las utilidades de IPMI, como IPMItool e ipmish

---

Puertos del iDRAC6

La Tabla 1-3 muestra una lista de los puertos en los que el iDRAC6 detecta las conexiones. La Tabla 1-4 identifica los puertos que el iDRAC6 usa como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un iDRAC6.

Tabla 1-3. Puertos en los que el iDRAC6 detecta servidores

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Redirección de consola teclado/ratón, Servicio de medios virtuales, Servicio seguro de medios virtuales, Video de redirección de consola

* Puerto configurable

Tabla 1-4. Puertos de cliente del iDRAC6

Número de puerto	Función
25	SMTP
53	DNS
68	Dirección IP asignada por DHCP
69	TFTP
162	Excepción SNMP
636	LDAPS
3269	LDAPS para catálogo global (GC)

Otros documentos útiles

Además de esta *Guía del usuario,* los siguientes documentos proporcionan información adicional sobre la configuración y funcionamiento del iDRAC6 en el sistema. Estos documentos están disponibles en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

- La ayuda en línea para el iDRAC6 proporciona información sobre el uso de la interfaz web.
- Consulte la *Guía del usuario de Dell Unified Server Configurator* para obtener más información sobre la configuración de servicios del sistema y hardware del iDRAC.
- La *Guía del usuario de Dell OpenManage IT Assistant* contiene información sobre cómo usar IT Assistant.
- Para instalar el iDRAC6, consulte *Manual del propietario de hardware*.
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- Para obtener información actualizada sobre las plataformas, los sistemas operativos y los exploradores web compatibles, consulte el archivo léame del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell*.
- La *Guía del usuario de Dell Update Packages* contiene información acerca de cómo obtener y usar Dell Update Packages como parte de su estrategia de actualización del sistema.
- Consulte la *Guía del usuario de utilidades del controlador de administración de la placa base de Dell OpenManage* para obtener información sobre el iDRAC6 y la interfaz IPMI.

Los siguientes documentos del sistema también están disponibles para ofrecer más información sobre el sistema en el que el iDRAC6 está instalado:

- En las instrucciones de seguridad suministradas con el sistema se proporciona información importante sobre normativas y seguridad. Para obtener más información sobre normativas, visite la página de inicio sobre cumplimiento de normativas en **www.dell.com/regulatory_compliance**. La información sobre la garantía puede estar incluida en este documento o constar en un documento aparte.
- En la *Guía de instalación del estante* incluida con la solución de estante se describe cómo instalar el sistema en un estante.
- En la *Guía de introducción* se ofrece una visión general sobre las funciones, la configuración y las especificaciones técnicas del sistema.
- En el *Manual del propietario de hardware* se proporciona información sobre las características del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.
- En la documentación del software de administración de sistemas se describen las funciones, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación del sistema operativo se describe cómo instalar (si es necesario), configurar y utilizar el software del sistema operativo.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- Algunas veces, con el sistema se incluyen actualizaciones que describen los cambios realizados en el sistema, en el software o en la documentación.

  NOTA: Lea siempre las actualizaciones primero, ya que a menudo éstas sustituyen la información de otros documentos.

- Es posible que se incluyan notas de la versión o archivos léame para proporcionar actualizaciones de última hora relativas al sistema o a la documentación, o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.

Regresar a la página de contenido

Regresar a la página de contenido

Introducción al iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

El iDRAC6 permite supervisar, solucionar problemas y reparar de manera remota un sistema Dell aun cuando el sistema esté apagado. El iDRAC6 ofrece un variado conjunto de funciones tales como la redirección de consola, medios virtuales, KVM virtual, autenticación con tarjeta inteligente e inicio de sesión único.

Management station es el sistema a partir del cual un administrador gestiona en forma remota un sistema Dell que cuenta con un iDRAC6. Los sistemas que son supervisados de este modo se denominan *sistemas administrados*.

En forma opcional, puede instalar el software OpenManage™ de Dell en su estación de administración, así como también en el sistema administrado. Sin el software de sistema administrado, usted no puede usar RACADM de manera local, y el iDRAC6 no puede capturar la pantalla de último bloqueo.

Para configurar el iDRAC6 debe seguir estos pasos generales:

NOTA: Este procedimiento puede ser distinto en varios sistemas. Consulte el *Manual del propietario del hardware* correspondiente al sistema específico en el sitio web de asistencia de Dell en **support.dell.com \ manuals** para ver instrucciones específicas sobre cómo realizar este procedimiento.

1. Configure las propiedades del iDRAC6, los valores de la red y los usuarios: puede configurar el iDRAC6 por medio de la utilidad de configuración del iDRAC6, la interfaz web o RACADM.
2. Si utiliza un sistema Windows, configure Microsoft® Active Directory® para proporcionar acceso al iDRAC6, que le permite agregar y controlar privilegios de usuarios del iDRAC6 a sus usuarios existentes en el software Active Directory.
3. Configure la autenticación con tarjeta inteligente: la tarjeta inteligente proporciona un nivel adicional de seguridad a la empresa.
4. Configure los puntos de acceso remoto, como la redirección de consola y los medios virtuales.
5. Configure los valores de seguridad.
6. Configure las alertas para la capacidad de administración eficiente de sistemas.
7. Configure los valores de la Interfaz de Administración de Plataforma Inteligente (IPMI) del iDRAC6 para utilizar las herramientas IPMI basadas en normas con el fin de administrar los sistemas de la red.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación básica de un iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección proporciona información sobre cómo instalar y configurar el hardware y software del iDRAC6.

Antes de comenzar

Reúna los siguientes elementos que se incluyen con el sistema, antes de instalar y configurar el software del iDRAC6:

- Hardware del iDRAC6 (ya instalado o en el paquete opcional)
- Procedimientos de instalación del iDRAC6 (incluidos en este capítulo)
- DVD *Dell Systems Management Tools and Documentation*

Instalación del hardware del iDRAC6 Express/Enterprise

NOTA: La conexión del iDRAC6 emula una conexión de teclado USB. Como resultado, cuando se reinicia el sistema, éste no le notificará si el teclado no está conectado.

El iDRAC6 Express/Enterprise puede estar preinstalado en su sistema, o disponible por separado. Para comenzar con el iDRAC6 que está instalado en su sistema, consulte "Generalidades de la instalación y configuración del software".

Si el iDRAC6 Express/Enterprise no está instalado en su sistema, consulte en el *Manual del propietario de hardware* de su plataforma las instrucciones de instalación del hardware.

Configuración de su sistema para usar el iDRAC6

Para configurar su sistema para usar un iDRAC6, use la utilidad de configuración para el iDRAC6.

Para ejecutar la utilidad de configuración para el iDRAC6:

1. Encienda o reinicie el sistema.
2. Pulse <Ctrl><E> cuando se le solicite durante la POST (Power-On Self- Test [autoprueba de encendido]).

   Si el sistema operativo comienza a cargarse antes de presionar <Ctrl><E>, espere a que el sistema termine de iniciarse y después reinicie el sistema e inténtelo de nuevo.
3. Configuración de LOM.
   a. Utilice las teclas de flecha para seleccionar los parámetros de la red de área local y presione <Entrar>. Se mostrará la selección de la tarjeta de interfaz de red.
   b. Use las teclas de flecha para seleccionar una de las siguientes opciones de modos de tarjeta de interfaz de red:
      - **Dedicada**: seleccione esta opción para activar el dispositivo de acceso remoto para utilizar la interfaz dedicada de red que está disponible en el iDRAC Enterprise. Esta interfaz no se comparte con el sistema operativo del host y encamina el tráfico de la administración hacia una red física separada, lo que permite separarlo del tráfico de aplicaciones. Esta opción sólo está disponible cuando el iDRAC6 Enterprise está instalado en el sistema.
      - **Compartida**: seleccione esta opción para compartir la interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de tarjetas de interfaz de red. El dispositivo de acceso remoto recibe datos por medio de la NIC 1 y la NIC 2, pero transmite datos sólo mediante la NIC 1. Si la NIC 1 falla, no se podrá acceder al dispositivo de acceso remoto.
      - **Compartida con fallo en LOM2**: seleccione esta opción para compartir la interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de tarjeta de interfaz de red. El dispositivo de acceso remoto recibe datos por medio de la NIC 1 y la NIC 2, pero transmite datos sólo mediante la NIC 1. Si la NIC 1 falla, el dispositivo de acceso remoto utilizará a la NIC 2 para la transmisión de todos los datos. El dispositivo de acceso remoto continúa usando la NIC 2 para la transmisión de datos. Si la NIC 2 falla, el dispositivo de acceso remoto fallará en todas las transmisiones de datos de regreso a la NIC 1 si el fallo en la NIC 1 se ha corregido.
      - **Compartida con fallo para todos los LOM**: seleccione esta opción para compartir la interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de tarjeta de interfaz de red. El dispositivo de acceso remoto recibe datos a través de la NIC 1, NIC 2, NIC 3 y NIC 4; pero sólo transmite datos por la NIC 1. Si la NIC 1 falla, el dispositivo de acceso remoto usa la NIC 2 para todas las transmisiones de datos.

Si la NIC 2 falla, el dispositivo de acceso remoto usa la NIC 3 para todas las transmisiones de datos. Si la NIC 3 falla, el dispositivo de acceso remoto usa la NIC 4 para todas las transmisiones de datos. Si la NIC 4 falla, el dispositivo de acceso remoto vuelve a usar la NIC 1 para todas las transmisiones de datos, pero sólo si la falla original en la NIC 1 se ha corregido. Es posible que esta opción no se encuentre disponible en el iDRAC6 Enterprise.

4. Configure los parámetros de la red de área local del controlador de red para usar DHCP o un origen de dirección IP estática.
   a. Usar la tecla de flecha hacia abajo para seleccionar **Parámetros de red de área local** y presione <Entrar>.
   b. Con las teclas de flecha hacia arriba y hacia abajo, seleccione **Origen de dirección IP**.
   c. Con las teclas de flecha derecha e izquierda, seleccione **DHCP**, **Auto Config o Estático**.
   d. Si seleccionó **Estático**, configure los valores de la **Dirección IP Ethernet**, la **Máscara de subred** y la **Puerta de enlace predeterminada**.
   e. Presione <Esc>.
5. Presione <Esc>.
6. Seleccione **Guardar los cambios y salir**.

Generalidades de la instalación y configuración del software

Esta sección ofrece una descripción de alto nivel de la instalación del software iDRAC6 y proceso de configuración. Para obtener más información acerca de los componentes del software iDRAC6, consulte "Instalación del software en el sistema administrado".

Instalación del software iDRAC6

Para instalar su software iDRAC6:

1. Instale el software en el sistema administrado. Consulte "Instalación del software en el sistema administrado".
2. Instale el software en la estación de administración. Consulte "Instalación del software en el sistema administrado".

Configuración de su iDRAC6

Para configurar su iDRAC6:

1. Use una de las siguientes herramientas de configuración:
   - Interfaz web (consulte "Configuración del iDRAC6 por medio de la interfaz web")
   - Interfaz de línea de comandos de RACADM (consulte "Uso de la interfaz de línea de comandos de SM-CLP del iDRAC6")
   - Consola de Telnet (consulte "Uso de una consola de Telnet")

   NOTA: Si usa más de una herramienta de configuración del iDRAC6 al mismo tiempo, podría obtener resultados inesperados.
2. Defina la configuración de red del iDRAC6. Consulte "Configuración de los valores de red del iDRAC6".
3. Agregue y configure usuarios del iDRAC6 Consulte "Cómo agregar y configurar usuarios del iDRAC6".
4. Configure el explorador web para acceder a la interfaz web. Consulte "Configuración de un explorador web admitido".
5. Desactive la opción de reinicio automático de Microsoft® Windows®. Consulte "Desactivación de la opción de reinicio automático de Windows".
6. Actualice el firmware del iDRAC6. Consulte "Actualización del firmware del iDRAC6".

Instalación del software en el sistema administrado

La instalación del software en el sistema administrado es opcional. Sin el software del sistema administrado, usted no puede usar RACADM de manera local, y el iDRAC6 no puede capturar la pantalla de último bloqueo.

Para instalar el software en el sistema administrado, utilice el DVD *Dell Systems Management Tools and Documentation*. Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida del software* disponible en el sitio web de asistencia de Dell: **support.dell.com\manuals**.

El software del sistema administrado instala las opciones de la versión adecuada de Dell™ OpenManage™ Server Administrator en el sistema administrado.

NOTA: No instale el software de estación de administración del iDRAC6 ni el software del sistema administrado del iDRAC6 en el mismo sistema.

Si Server Administrator no está instalado en el sistema administrado, usted no podrá ver la pantalla de último bloqueo del sistema ni usar la función de **Recuperación automática**.

Para obtener más información sobre la pantalla de último bloqueo, consulte "Cómo ver la pantalla de último bloqueo del sistema".

Instalación del software en la estación de administración

El sistema incluye el DVD *Dell Systems Management Tools and Documentation*. Este DVD ofrece los siguientes componentes:

- Directorio raíz del DVD: contiene Dell Systems Build and Update Utility, que proporciona información sobre la instalación y configuración del servidor y del sistema.
- SYSMGMT: contiene productos de software de administración de sistemas, incluido Dell OpenManage Server Administrator
- Docs: contiene documentación para productos de software de administración de sistemas, periféricos y controladores RAID
- SERVICE: contiene las herramientas que necesita para configurar el sistema, y cuenta con los últimos diagnósticos y controladores optimizados por Dell para el sistema

Para obtener información sobre Server Administrator, IT Assistant y Unified Server Configurator, vea la *Guía del usuario de Server Administrator*, la *Guía del usuario de IT Assistant* y la *Guía del usuario de Unified Server Configurator* disponibles en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

Instalación y desinstalación de RACADM en una estación de administración de Linux

Para usar las funciones de RACADM remota, instale RACADM en una estación de administración que ejecuta Linux.

NOTA: Cuando se ejecuta el programa **Setup** del DVD *Dell Systems Management Tools and Documentation*, se instala la utilidad RACADM para todos los sistemas operativos compatibles en la estación de administración.

Instalación de RACADM

1. Inicie sesión como usuario "root" en el sistema en donde desea instalar los componentes de la estación de administración.
2. De ser necesario, monte el DVD *Dell Systems Management Tools and Documentation* con el comando siguiente o un comando similar:

   ```
   mount /media/cdrom
   ```

3. Diríjase al directorio **/linux/rac** y ejecute el comando siguiente:

   ```
   rpm -ivh *.rpm
   ```

Para recibir ayuda con el comando RACADM, escriba **racadm help** después de enviar los comandos anteriores.

Desinstalación de RACADM

Para desinstalar RACADM, abra una petición de comandos y escriba:

```
rpm -e <nombre_del_paquete_de_racadm>
```

donde <*nombre_del_paquete_de_racadm*> es el paquete RPM que se usó para instalar el software del RAC.

Por ejemplo, si el nombre del paquete RPM es **srvadmin-racadm5**, escriba:

```
rpm -e srvadmin-racadm5
```

Actualización del firmware del iDRAC6

Utilice uno de los métodos siguientes para actualizar el firmware del iDRAC6.

- Interfaz web (consulte "Actualización del firmware del iDRAC6 mediante la interfaz web")
- Interfaz de línea de comandos de RACADM (consulte "Actualización del firmware del iDRAC6 mediante RACADM")
- Dell Update Packages (consulte "Actualización del firmware del iDRAC6 mediante Dell Update Packages para sistemas operativos Windows y Linux compatibles")

Antes de comenzar

Antes de actualizar el firmware del iDRAC6 con RACADM local o Dell Update Packages, realice los siguientes procedimientos. De lo contrario, podría fallar la operación de actualización del firmware.

1. Instale y active los controladores de nodo administrado y la IPMI correspondientes.
2. Si el sistema ejecuta un sistema operativo Windows, active e inicie el servicio **Instrumental de administración de Windows** (WMI).
3. Si usa el iDRAC6 Enterprise en un sistema con SUSE® Linux Enterprise Server (versión 10) para Intel® EM64T, inicie el servicio **Raw**.
4. Desconecte y desmonte los medios virtuales.

   NOTA: Si las actualizaciones de firmware del iDRAC6 se interrumpen por cualquier motivo, podrá necesitar esperar hasta 30 minutos antes de que se permita otra actualización de firmware.

5. Compruebe que el USB esté activado.

Descargue el firmware del iDRAC6

Para actualizar el firmware del iDRAC6, descargue el firmware más reciente del sitio web de asistencia de Dell en **support.dell.com** y guarde el archivo en el sistema local.

En el paquete de firmware del iDRAC6 se incluyen los componentes de software siguientes:

- Datos y código de firmware compilado del iDRAC6
- Interfaz web, archivos JPEG y otros archivos de datos de la interfaz de usuario
- Archivos de configuración predeterminados

Actualización del firmware del iDRAC6 mediante la interfaz web

Para obtener más información, consulte "Actualización del firmware del iDRAC6/imagen de recuperación de los servicios del sistema".

Actualización del firmware del iDRAC6 mediante RACADM

Puede actualizar el firmware del iDRAC6 mediante la herramienta RACADM de interfaz de línea de comandos. Si ha instalado Server Administrator en el sistema administrado, utilice RACADM local para actualizar el firmware.

1. Puede descargar la imagen del firmware del iDRAC6 en el sistema administrado a través del sitio web de asistencia técnica de Dell: **support.dell.com**.

   Por ejemplo:

   ```
   C:\downloads\firmimg.d6
   ```

2. Ejecute el siguiente comando RACADM:

   ```
   racadm fwupdate -pud c:\downloads\
   ```

   También puede actualizar el firmware usando RACADM remoto y un servidor TFTP.

   Por ejemplo:

   racadm -r <*dirección IP del iDRAC6*> -u <*nombre de usuario*> -p <*contraseña*> fwupdate -g -u -a <*ruta de acceso*>

   donde *ruta de acceso* es la ubicación en el servidor TFTP en la que está almacenado **firmimg.d6**.

Actualización del firmware del iDRAC6 mediante Dell Update Packages para sistemas operativos Windows y Linux compatibles

Para descargar y ejecutar los paquetes Dell Update Packages para sistemas operativos Windows y Linux compatibles, visite el sitio web de asistencia de Dell: **support.dell.com**. Para obtener más información, consulte la *Guía del usuario de Dell Update Package* que se encuentra en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

NOTA: Cuando actualice el firmware del iDRAC6 usando la utilidad Dell Update Package en Linux, podrá ver los siguientes mensajes en la consola:

```
usb 5-2: device descriptor read/64, error -71

usb 5-2: device descriptor not accepting address 2, error -71
```

La naturaleza de estos mensajes es puramente estética y deben ser ignorados. Estos mensajes se deben a que los dispositivos USB se han restablecido durante el proceso de actualización del firmware y son inofensivos.

Cómo borrar la caché del explorador

Después de actualizar el firmware, borre la caché del explorador web.

Consulte la ayuda en línea del explorador web para obtener más información.

Configuración de un explorador web admitido

Las secciones siguientes proporcionan instrucciones para configurar los exploradores web admitidos.

Configuración del explorador web para conectarse a la interfaz web del iDRAC6

Si se conecta a la interfaz web del DRAC6 desde una estación de administración conectada a Internet mediante un servidor proxy, debe configurar el explorador web para que acceda a Internet desde este servidor.

Para configurar el explorador web Internet Explorer para tener acceso al servidor proxy:

1. Abra una ventana del explorador web.
2. Haga clic en **Herramientas** y haga clic en **Opciones de Internet**.
3. En la ventana **Opciones de Internet**, haga clic en la lengüeta **Conexiones**.
4. En **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
5. Si la casilla **Usar un servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.
6. Haga clic dos veces en **Aceptar**.

Lista de dominios de confianza

Cuando se accede a la interfaz web del iDRAC6 por medio del explorador web, se le pedirá agregar la dirección IP del iDRAC6 a la lista de dominios de confianza si la dirección IP no aparece en la lista. Al terminar, haga clic en Actualizar o reinicie el explorador web para restablecer la conexión con la interfaz web del iDRAC6.

Exploradores web de 32 bits y 64 bits

La interfaz web del iDRAC6 no se admite en los exploradores web de 64 bits. Si abre un explorador de 64 bits, accede a la página de redirección de consola e intenta instalar el complemento, el procedimiento fallará. Si este error no se reconoce y se repite este procedimiento, la página de redirección de consola se cargará aun cuando la instalación del complemento haya fallado durante el primer intento. Este problema se presenta porque el explorador web guarda la información del complemento en el directorio del perfil aun cuando el procedimiento de instalación del complemento haya fallado. Para resolver este problema, instale y ejecute un explorador web de 32 bits admitido e inicie sesión en el iDRAC6.

Visualización de versiones localizadas de la interfaz web

Windows

La interfaz web del iDRAC6 es compatible con los siguientes idiomas de sistemas operativos Windows:

- Inglés
- Francés
- Alemán
- Español
- Japonés
- Chino simplificado

Para ver una versión traducida de la interfaz web del iDRAC6 en Internet Explorer:

1. Haga clic en el menú **Herramientas** y seleccione **Opciones de Internet**.
2. En la ventana **Opciones de Internet**, haga clic en **Idiomas**.
3. En la **ventana Preferencias de idioma**, haga clic en **Agregar**.
4. En la ventana **Agregar idioma**, seleccione un idioma compatible.

   Para seleccionar más de un idioma, presione <Ctrl>.
5. Seleccione el idioma de su preferencia y haga clic en **Subir** para subir el idioma a la parte superior de la lista.
6. Haga clic en **Aceptar**.
7. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.

Linux

Si ejecuta la redirección de consola en un cliente con Red Hat® Enterprise Linux® (versión 4) con interfaz gráfica en chino simplificado, es posible que el menú del visor y el título muestren caracteres aleatorios. Este problema se debe a una codificación incorrecta en el sistema operativo Red Hat Enterprise Linux (versión 4) en chino simplificado. Para resolver este problema, acceda a la configuración de codificación actual y modifíquela por medio de los siguientes pasos:

1. Abra una ventana de terminal de comandos.
2. Escriba "locale" y presione <Entrar>. Se muestra la siguiente información:

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Si los valores incluyen "zh_CN.UTF-8", no es necesario hacer cambios. Si los valores no incluyen "zh_CN.UTF-8", vaya al paso 4.
4. Diríjase al archivo **/etc/sysconfig/i18n**.
5. En el archivo, aplique los cambios siguientes:

   Entrada actual:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

   Entrada actualizada:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6. Cierre sesión y después inicie sesión en el sistema operativo.
7. Reinicie el iDRAC6.

Cuando cambie de cualquier otro idioma al chino simplificado, asegúrese que este ajuste siga siendo válido. Si no es así, repita este procedimiento.

Para ver las configuraciones avanzadas del iDRAC6, consulte "Configuración avanzada del iDRAC6".

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del iDRAC6 por medio de la interfaz web

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

El iDRAC6 ofrece una interfaz web que permite configurar las propiedades y usuarios del iDRAC6, realizar tareas de administración remota y solucionar problemas de un sistema (administrado) remoto. Para la administración diaria de sistemas, use la interfaz web del iDRAC6. Este capítulo proporciona información sobre cómo realizar tareas comunes de administración de sistemas con la interfaz web del iDRAC6 y proporciona vínculos con información relacionada.

La mayor parte de las tareas de configuración de interfaz pueden realizarse con comandos racadm u otros comandos del protocolo de línea de comandos para la administración de servidores (SM-CLP).

Los comandos de RACADM local se ejecutan desde el servidor administrado.

Los comandos de SM-CLP y SSH/Telnet RACADM se ejecutan en un shell al que se puede tener acceso de manera remota con una conexión Telnet o SSH. Para obtener más información sobre SM-CLP, consulte "Uso de la interfaz de línea de comandos de SM-CLP del iDRAC6". Para obtener más información sobre comandos RACADM, consulte "Generalidades de los subcomandos de RACADM" y "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

Acceso a la interfaz web

Para acceder a la interfaz web del iDRAC6, realice los pasos que se indican a continuación:

1. Abra una ventana de un explorador web compatible.

   Consulte "Exploradores web admitidos" para obtener más información.

   Para acceder a la interfaz web utilizando una dirección IPv4, diríjase al paso 2

   Para acceder a la interfaz web utilizando una dirección IPv6, diríjase al paso 3

2. Para acceder a la interfaz web utilizando una dirección IPv4, debe tener IPv4 activada:

   En la barra de **Dirección** del explorador, escriba:

   https://<dirección IPv4 del iDRAC>

   Luego, presione <Entrar>.

3. Para acceder a la interfaz web utilizando una dirección IPv6, debe tener IPv6 activada:

   En la barra de **Dirección** del explorador, escriba:

   https://[<dirección IPv6 del iDRAC>]

   Luego, presione <Entrar>.

4. Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<dirección_IP_de_iDRAC>:<número_de_puerto>

   donde *dirección_IP_de_iDRAC es la dirección IP del iDRAC6 y número_de_puerto* es el número del puerto HTTPS.

5. En el campo **Dirección**, escriba https://<dirección_IP_de_iDRAC> y presione <Entrar>.

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<*dirección_IP_de_iDRAC*>:<*número_de_puerto*>

   donde *dirección_IP_de_iDRAC* es la dirección IP del iDRAC6 y *número_de_puerto* es el número del puerto HTTPS.

Aparecerá la ventana **Inicio de sesión** del iDRAC6.

Inicio de sesión

Puede iniciar sesión como usuario del iDRAC6 o como usuario de Microsoft® Active Directory®. El usuario y la contraseña predeterminados para un usuario del iDRAC6 son **root** y **calvin**, respectivamente.

Para que pueda iniciar sesión en el iDRAC, el administrador debe haberle otorgado privilegio de **Inicio de sesión en el iDRAC.**

Para iniciar sesión, realice los pasos siguientes:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes valores:
   - Su nombre de usuario del iDRAC6.

     En el nombre de usuario para los usuarios locales se distingue entre mayúsculas y minúsculas. Algunos ejemplos son `root`, `usuario_de_TI` o `juan_perez`.
   - Su nombre de usuario de Active Directory.

     Los nombres de Active Directory se pueden introducir en cualquiera de los formatos *<nombre_de_usuario>*, *<dominio>**<nombre_de_usuario>*, *<dominio>*/*<nombre_de_usuario>*o *<usuario>*@*<dominio>*. En ellos no se distingue entre mayúsculas y minúsculas. Algunos ejemplos son `dell.com\juan_perez`, o `JUAN_PEREZ@DELL.COM`.
2. En el campo **Contraseña**, escriba la contraseña de usuario del iDRAC6 o la contraseña de usuario de Active Directory. Las contraseñas distinguen entre mayúsculas y minúsculas.
3. Desde el casillero **Dominio**, seleccione *Este iDRAC* para iniciar sesión como usuario del iDRAC6 o seleccione cualquier dominio disponible para iniciar sesión como un usuario de Active Directory.

   NOTA: Para los usuarios de Active Directory, si usted especificó un nombre de dominio como parte del nombre de usuario, seleccione *Este iDRAC* desde el menú desplegable.
4. Haga clic en **Aceptar** o presione <Entrar>.

Cierre de sesión

1. En la esquina superior derecha de la ventana principal, haga clic en **Cerrar sesión** para cerrar la sesión.
2. Cierre la ventana del explorador.

NOTA: El botón **Cerrar sesión** no aparecerá a menos que usted haya iniciado sesión.

NOTA: Si cierra el explorador sin cerrar sesión de manera ordenada puede provocar que la sesión permanezca abierta hasta que expire el tiempo. Se recomienda enfáticamente que haga clic en el botón de cierre de sesión para terminar la sesión; de lo contrario, la sesión puede permanecer activa hasta que expire el tiempo de la sesión.

NOTA: Cerrar la interfaz web del iDRAC6 en Microsoft Internet Explorer mediante el botón para cerrar ("x"), que se encuentra en la esquina superior derecha de la ventana, podría generar un error de aplicación. Para resolver este problema, descargue la actualización de seguridad acumulativa más reciente para Internet Explorer desde el sitio web de asistencia de Microsoft, en **support.microsoft.com**.

Configuración de la tarjeta de interfaz de red del iDRAC6

Esta sección supone que el iDRAC6 ya ha sido configurado y se puede tener acceso al mismo en la red. Consulte "Configuración de su iDRAC6" para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de LAN de IPMI y de red

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC**.

NOTA: La mayoría de los servidores DHCP requieren un servidor para guardar un símbolo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este símbolo durante la negociación de DHCP. El iDRAC6 proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

NOTA: Si usted utiliza el protocolo de árbol de expansión (STP) activado, asegúrese de que también tiene PortFast o una tecnología similar en funcionamiento de la siguiente forma:

- En los puertos para el interruptor conectados al iDRAC6
- En los puertos conectados a la estación de administración con una sesión KVM del iDRAC

NOTA: Podría ver el siguiente mensaje si el sistema se detiene durante la POST (Power-On Self-Test [autoprueba de encendido]): Strike the F1 key to continue, F2 to run the system setup program (Presione la tecla F1 para continuar, F2 para ejecutar el programa de configuración del sistema.) Una posible razón del error es un inconveniente de red que cause pérdida de comunicación con el iDRAC6. Después de que el inconveniente de red se solucione, reinicie el sistema.

1. Haga clic en **Acceso Remoto**→ **Configuración**→ **Usuarios**.
2. En la página **Red**, puede ingresar en las configuraciones de la tarjeta de interfaz de red, configuraciones comunes del iDRAC, configuraciones IPv4, IPv6, IPMI y VLAN. Consulte la Tabla 4-1, la Tabla 4-2, la Tabla 4-3, la tabla 4-4, la Tabla 4-5 y la Tabla 4-6 para obtener descripciones de estos valores de configuración.

3. Cuando haya terminado de introducir los valores necesarios, haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-7.

Tabla 4-1. Configuración de tarjeta de interfaz de red

Valor	Descripción
Selección de NIC	Configura el modo actual según los cuatro modos posibles · Dedicado (iDRAC NIC) **NOTA:** Esta opción sólo está disponible en el iDRAC6 Enterprise. · Compartido (LOM1) · Compartido con LOM2 de protección contra fallas · Compartido con todos los LOM2 de protección contra fallas **NOTA:** Es posible que esta opción no se encuentre disponible en el iDRAC6 Enterprise. **NOTA:** El iDRAC6 no se comunicará localmente a través del mismo puerto físico si la opción **Selección de NIC** está establecida en los modos **Compartido** o **Compartido con protección contra fallas**. Esto se debe a que un conmutador de red no enviará paquetes a través del mismo puerto en el que los recibió.
Dirección MAC	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red.
Activar NIC	Cuando se selecciona, indica que el NIC está activado y habilita los controles restantes en este grupo. Cuando un NIC está desactivado, toda la comunicación hacia el iDRAC6 y que provenga del mismo a través de la red está bloqueada. El valor predeterminado es **activado**.
Negociar automáticamente	Si está **activado**, muestra la velocidad de red y modo al comunicarse con el router o hub más cercano. Si está **desactivado**, permite configurar la velocidad de red y el modo dúplex de forma manual (desactivado) Si **Selección de NIC** *no* está establecida en **Dedicada**, la configuración de negociación automática siempre estará **activada**.
Velocidad de red	Le permite configurar la velocidad de red a 100 Mb o 10 Mb para coincidir con su entorno de red. Esta opción no está disponible si la negociación automática se ha establecido como **Activada**.
Modo dúplex	Establezca el valor del modo dúplex en completo o medio para que coincida con el entorno de red. Esta opción no está disponible si la **negociación automática** se ha establecido como **Activada**.

Tabla 4-2. Configuración común del iDRAC

Valor	Descripción
Registrar el iDRAC en DNS	Registra el nombre del iDRAC6 en el servidor DNS. El valor predeterminado es **Desactivado**.
Nombre del iDRAC en DNS	Muestra el nombre del iDRAC6 únicamente cuando la opción **Registrar el iDRAC en DNS** está seleccionada. El nombre predeterminado es idrac-*etiqueta_de_servicio*, donde *etiqueta_de_servicio* es el número de la etiqueta de servicio del servidor Dell. Por ejemplo: idrac-00002
Usar DHCP para el nombre del dominio de DNS	Utiliza el nombre de dominio de DNS predeterminado. Cuando la casilla no está seleccionada y la opción **Registrar el iDRAC en DNS** está seleccionada, usted puede modificar el nombre de dominio de DNS en el campo **Nombre de dominio de DNS**. El valor predeterminado es **Desactivado**. **NOTA:** Para seleccionar la casilla **Usar DHCP para el nombre de dominio de DNS**, seleccione también la casilla **Usar DHCP (para la dirección IP de NIC)**.
Nombre de dominio de DNS	El **nombre de dominio de DNS** predeterminado está en blanco. Cuando la casilla **Usar DHCP para el nombre de dominio de DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.

Tabla 4-3. Configuración de IPv4

Valor	Descripción
Activado	Si la NIC está activada, esto selecciona la compatibilidad con el protocolo IPv4 y activa los demás campos en este sección.
Usar DHCP (para la dirección IP de la tarjeta de interfaz de red)	Pide al iDRAC6 que obtenga una dirección IP para la NIC del servidor de protocolo de configuración dinámica de host (DHCP). El valor predeterminado es **desactivado**.

Dirección IP	Especifica la dirección IP de la NIC del iDRAC6.
Máscara de subred	Permite introducir o editar una dirección IP estática para la NIC del iDRAC6. Para cambiar este valor, deje en blanco la casilla Usar DHCP (para la dirección IP de la tarjeta de interfaz de red).
Puerta de enlace	Dirección de un router o un conmutador. El valor se muestra en formato de números separados con puntos, por ejemplo, 192.168.0.1.
Usar DHCP para obtener direcciones de servidores DNS	Habilite el DHCP para obtener direcciones de servidores DNS por medio de la selección de la casilla **Usar DHCP para obtener direcciones de servidores DNS**. Cuando no se usa DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**. El valor predeterminado es **desactivado**. **NOTA:** Cuando la casilla **Usar DHCP para obtener direcciones de servidores DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Dirección IP del servidor DNS
Servidor DNS alternativo	Dirección IP alternativa.

Tabla 4-4. Configuración de IPv6

Valor	Descripción
Activado	Si la casilla está seleccionada, IPv6 está activado. Si la casilla no está seleccionada, IPv6 está desactivado. El valor predeterminado es desactivado.
Auto Config	Marcar este casilla le permite al iDRAC6 obtener la dirección IPv6 para la NIC del iDRAC6 desde el servidor del protocolo de configuración dinámica de host (DHCP). Activar **Auto Config** también desactiva y hace salir los valores estáticos para dirección IP 1, longitud de prefijo y puerta de enlace IP.
Dirección IP 1	Especifica la dirección IPv6 para la NIC del iDRAC Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Longitud de prefijo	Configura la longitud de prefijo de la dirección IPv6. Se puede valuar entre 1 y 128 inclusive. Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Puerta de enlace IP	Configura la puerta de enlace estática para la NIC del iDRAC. Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Dirección local de vínculo	Especifica la dirección IPv6 de la NIC del iDRAC6.
Dirección IP 2	Especifica la dirección IPv6 adicional de la NIC del iDRAC6, si hay una disponible.
Usar DHCP para obtener direcciones de servidores DNS	Habilite el DHCP para obtener direcciones de servidores DNS por medio de la selección de la casilla **Usar DHCP para obtener direcciones de servidores DNS**. Cuando no se usa DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**. El valor predeterminado es desactivado. Verifique la copia de revisión NOTA: Cuando la casilla **Usar DHCP para obtener direcciones de servidores DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Especifica la dirección IPv6 estática del servidor DNS preferido. Para cambiar esta configuración, debe primero deseleccionar **Usar DHCP para obtener direcciones de servidores DNS.**
Servidor DNS alternativo	Especifica la dirección IPv6 estática del servidor DNS alternativo. Para cambiar esta configuración, debe primero deseleccionar **Usar DHCP para obtener direcciones de servidores DNS.**

Tabla 4-5. Configuración de IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando está seleccionado, indica que el canal LAN de IPMI está activado. El valor predeterminado es **desactivado**.
Límite del nivel de privilegios del canal	Configura el nivel mínimo de privilegios del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: **Administrador**, **Operador** o **Usuario**. El valor predeterminado es **Administrador**.
Clave de cifrado	Configura la clave de cifrado: de 0 a 20 caracteres hexadecimales (no se permiten espacios). De manera predeterminada está en blanco.

Tabla 4-6. Configuración de VLAN

Valor	Descripción
Activar identificación de VLAN	Si está activada, solo tráfico con identificación de LAN virtual (VLAN) coincidente será aceptado.
Identificación de VLAN	Campo Identificación de VLAN de campos de 802.1g. Un valor válido para la identificación de VLAN virtual debe ser un número entre 1 y 4094.
Prioridad	Campo Prioridad de campos de 802.1g. Introduzca un número entre 0 y 7 para establecer la prioridad de identificación de VLAN.

Tabla 4-7. Botones de la página de configuración de la red

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de red**.
Configuración avanzada	Abre la página **Seguridad de la red** y permite al usuario introducir atributos del rango de IP y de bloqueo de IP.
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la página de configuración de la red. **NOTA:** Si se hacen cambios en la configuración de la dirección IP de la NIC se cerrarán todas las sesiones de usuario y los usuarios tendrán que volver a conectarse a la interfaz web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requerirán que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración de la filtración de IP y el bloqueo de IP

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC**.

1. Haga clic en **Acceso remoto**→ **Configuración** y luego en la lengüeta **Red** para abrir la página **Red**.
2. Haga clic en **Configuración avanzada** para configurar los valores de seguridad de la red.

   La Tabla 4-8 describe los **valores de la página Seguridad de la red**. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.
3. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-9.

Tabla 4-8. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango de IP, que define un rango de direcciones IP que puede acceder al iDRAC. El valor predeterminado es **desactivado**.
Dirección del rango de IP	Determina el patrón de bits aceptable de la dirección IP, en función de los números 1 de la máscara de subred. Este valor es bitwise AND'd con la máscara de subred del rango IP para determinar la parte superior de una dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el iDRAC6.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. El valor predeterminado es **255.255.255.0**.
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido. El valor predeterminado es **desactivado**.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección. El valor predeterminado es **10**.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. El valor predeterminado es **3600.**

Tabla 4-9. Botones de la página de seguridad de la red

Botón	Descripción
Imprimir	Imprime los valores de la **Seguridad de la red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Seguridad de la red**
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la página **Seguridad de la red**.
Regresar a la página Configuración de red.	Regresa a la página **Configuración de red**.

Configuración de los eventos de plataforma

La configuración de eventos de plataforma ofrece un mecanismo para configurar el iDRAC6 a fin de realizar las acciones seleccionadas ante ciertos mensajes de eventos. Las acciones incluyen reiniciar el sistema, sin acción, realizar ciclo de encendido del sistema, apagar el sistema y generar una alerta (excepción de eventos de plataforma [PET] y/o correo electrónico).

Los eventos de plataforma que se pueden filtrar se muestran en la Tabla 4-10.

Tabla 4-10. Filtros de eventos de plataforma

Índice	Evento de plataforma
1	Declaración crítica del ventilador
2	Declaración de advertencia de la batería
3	Declaración crítica de la batería
4	Declaración crítica de voltaje discreto
5	Declaración de advertencia de temperatura
6	Declaración crítica de temperatura
7	Declaración crítica de intrusión
8	Redundancia del ventilador degradada
9	Redundancia del ventilador perdida
10	Declaración de advertencia del procesador
11	Declaración crítica del procesador
12	Procesador ausente
13	Declaración de advertencia de suministro de energía
14	Declaración crítica de suministro de energía
15	Suministro de energía ausente
16	Declaración crítica de registro de eventos
17	Declaración crítica de vigilancia
18	Declaración de advertencia de alimentación del sistema
19	Declaración crítica de alimentación del sistema

.

Cuando se presenta un evento de plataforma (por ejemplo, una declaración de advertencia de la batería), se genera un evento de sistema y se registra en el registro de eventos del sistema (SEL). Si este evento coincide con un filtro de eventos de plataforma (PEF) que está activado, y usted ha configurado el filtro para generar una alerta (PET o correo electrónico), se enviará una alerta por correo electrónico o PET a uno o más destinos configurados.

Si el mismo filtro de eventos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecutará.

Configuración de los filtros de eventos de plataforma (PEF)

NOTA: Configure los filtros de eventos de plataforma antes de configurar excepciones de eventos de plataforma o alertas por correo electrónico.

1. Inicie sesión en el sistema remoto por medio de un explorador web admitido. Consulte "Acceso a la interfaz web".
2. Haga clic en **Sistema**→ **Manejo de alertas**→ **Eventos de plataforma**.
3. En la primera tabla, seleccione **Permitir alertas del filtro de eventos de plataforma** y luego haga clic en **Aplicar cambios**.

   NOTA: Permitir alertas del filtro de eventos de plataforma deberá estar activado para que se envíe una alerta a cualquier destino válido configurado (PET o correo electrónico).

4. En la próxima tabla, **Lista de filtros de eventos de plataforma**, haga clic en el filtro que quiera configurar.
5. En la página **Configurar eventos de plataforma**, seleccione la **Acción de apagado** apropiada o seleccione **Ninguna**.
6. Seleccione o deseleccione **Generar alerta** para activar o desactivar esta acción.

   NOTA: Generar alerta deberá estar activado para que se envíe una alerta a cualquier destino válido configurado (PET o correo electrónico).

7. Haga clic en **Aplicar cambios**.

   Regresará a la página **Eventos de plataforma**, donde los cambios que usted realizó se muestran en la **Lista de filtros de eventos de plataforma.**

8. Repita los pasos del 4 al 7 para configurar filtros de eventos de plataforma adicionales.

Configuración de excepciones de eventos de plataforma (PET)

NOTA: Debe tener permiso para **Configurar el iDRAC** para poder agregar, activar o desactivar una alerta SNMP. Las opciones siguientes no estarán disponibles si no tiene permiso para **Configurar el iDRAC**.

1. Inicie sesión en el sistema remoto por medio de un explorador web admitido. Consulte "Acceso a la interfaz web".
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de eventos de plataforma (PEF)".
3. Haga clic en **Sistema**→ **Manejo de alertas**→ **Configuración de excepciones**.
4. En las opciones **Lista de destinos IPv4** o **Lista de destinos IPv6**, haga clic en un número de destino para configurar el destino de las alertas SNMP de IPv4 o IPv6.
5. En la página **Configurar destino de alerta de eventos de plataforma**, seleccione o deseleccione **Activar destino**. Una casilla seleccionada indica que la dirección IP está activada para recibir las alertas. Una casilla no seleccionada indica que la dirección IP está desactivada para recibir las alertas.
6. Introduzca una dirección IP de destino válida de excepción de eventos de plataforma y haga clic en **Aplicar cambios**.
7. Haga clic en **Enviar excepción de prueba** para verificar la alerta configurada o haga clic en **Regresar a la página de destino de eventos de plataforma.**

   NOTA: Su cuenta de usuario debe tener permiso para **Probar alertas** para enviar una excepción de prueba. Consulte la Tabla 6-6, "Permisos de grupos del iDRAC", para obtener más información.

   En la página **Destinos de alerta de eventos de plataforma**, los cambios aplicados se muestran en la **Lista de destino** de IPv4 y de IPv6.
8. En el campo **Cadena de comunidad**, introduzca el nombre de comunidad SNMP del iDRAC apropiado. Haga clic en **Aplicar cambios**.

   NOTA: La cadena de la comunidad de destino debe ser la misma que la cadena de la comunidad del iDRAC6.
9. Repita los pasos del 4 al 7 para configurar números de destino adicionales de IPv4 o IPv6.

Configuración de alertas por correo electrónico

NOTA: Alertas por correo electrónico que admiten direcciones IPv4 e IPv6.

1. Inicie sesión en el sistema remoto por medio de un explorador web admitido.
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de eventos de plataforma (PEF)".
3. Haga clic en **Sistema**→ **Manejo de alertas**→ **Configuración de alertas por correo electrónico**.
4. En la tabla debajo de **Direcciones de correo electrónico de destino**, haga clic en el **número de alerta de correo electrónico** para la que desea configurar la dirección de destino.
5. En la página **Configurar alerta por correo electrónico**, seleccione o deseleccione **Activar alerta por correo electrónico.** Una casilla seleccionada indica que la dirección IP está activada para recibir las alertas. Una casilla no seleccionada indica que la dirección IP está desactivada para recibir las alertas.
6. En el campo **Dirección de correo electrónico de destino**, escriba una dirección válida de correo electrónico.
7. En el campo **Descripción de correo electrónico**, escriba una breve descripción de lo que se mostrará en el correo electrónico.
8. Haga clic en **Aplicar cambios.**
9. Si desea verificar la alerta de correo electrónico configurada, haga clic en **Enviar correo electrónico de prueba**. Si no lo desea, haga clic en **Regresar a la página de destino de alertas por correo electrónico.**
10. Haga clic en **Regresar a la página de destino de alertas por correo electrónico** e introduzca una dirección IP de SMTP válida en el campo **Dirección IP del servidor SMTP (correo electrónico)**.

    NOTA: Para enviar un correo electrónico de prueba exitosamente, **la dirección IP del servidor SMTP (correo electrónico)** debe configurarse en la página **Configuraciones de alertas por correo electrónico.** El servidor SMTP utiliza la dirección IP establecida para comunicarse con el iDRAC6 para enviar alertas por correo electrónico cuando un evento de plataforma ocurra.
11. Haga clic en **Aplicar cambios**.
12. Repita los pasos del 4 al 9 para configurar destinos de alertas por correo electrónico adicionales.

Configuración de IPMI

1. Inicie sesión en el sistema remoto por medio de un explorador web admitido.

2. Configure la IPMI en la LAN.

   a. En el árbol **Sistema**, haga clic en **Acceso remoto**.

   b. Haga clic en la lengüeta **Configuración** y haga clic en **Red**.

   c. En la página **Configuración de red** en **Configuración de LAN de IPMI**, seleccione **Activar IPMI en la LAN** y haga clic en **Aplicar cambios**.

   d. Actualice los privilegios del canal de LAN de IPMI, si es necesario.

   NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

   En **Configuración de LAN de IPMI**, haga clic en el menú desplegable **Límite de nivel de privilegios del canal**, seleccione **Administrador**, **Operador** o **Usuario** y haga clic en **Aplicar cambios**.

   e. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

   NOTA: La IPMI del iDRAC6 es compatible con el protocolo RMCP+.

   En **Configuración de LAN de IPMI** en el campo **Clave de cifrado**, escriba la clave de cifrado y haga clic en **Aplicar cambios**.

   NOTA: La clave de cifrado debe consistir en un número par de caracteres hexadecimales con un máximo de 40 caracteres.

3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

   a. En el árbol **Sistema**, haga clic en **Acceso remoto**.

   b. En la lengüeta **Configuración**, haga clic en **Comunicación en serie en la LAN**.

   c. En la página **Configuración de la comunicación en serie en la LAN**, seleccione **Activar comunicación en serie en la LAN**.

   d. Actualice la velocidad en baudios de la SOL de IPMI.

   NOTA: Para redirigir la consola serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

   e. Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

   f. Actualice el **Privilegio mínimo requerido.** Esta propiedad define el privilegio mínimo de usuario que se requiere para usar la función **Comunicación en serie en la LAN**.

   Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Usuario**, **Operador** o **Administrador**.

   g. Haga clic en **Aplicar cambios**.

4. Configure la conexión serie de IPMI.

   a. En la lengüeta **Configuración**, haga clic en **Serie**.

   b. En el menú **Configuración serie**, cambie el modo de la conexión serie de IPMI al valor adecuado.

   En **Conexión serie de IPMI**, haga clic en el menú desplegable **Valor del modo de conexión** y seleccione el modo adecuado.

   c. Establezca la velocidad en baudios de la conexión serie de IPMI.

   Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

   d. Establezca el límite del nivel de privilegios de canal.

   Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Administrador**, **Operador** o **Usuario**.

   e. Haga clic en **Aplicar cambios**.

   f. Compruebe que el multiplexor serie esté configurado correctamente en el programa de configuración del BIOS del sistema administrado.

      - Reinicie el sistema.
      - Durante la POST (Power-On Self-Test [autoprueba de encendido]), presione <F2> para ingresar al programa de configuración del BIOS.
      - Diríjase a **Comunicación serie**.
      - En el menú **Conexión serie**, compruebe que **Conector serie externo** esté definido como **Dispositivo de acceso remoto**.
      - Guarde los cambios y salga del programa de configuración del BIOS.
      - Reinicie el sistema.

Si la conexión serie de IPMI está en modo de terminal, puede configurar los siguientes valores adicionales:

- Control de eliminación

- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0. Para obtener información adicional acerca de comandos de modo terminal, consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* en **support.dell.com\manuals**\.

Configuración de usuarios del iDRAC6

Para obtener más información, consulte "Cómo agregar y configurar usuarios del iDRAC6".

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales

Esta sección ofrece información sobre las funciones de seguridad de datos siguientes que vienen incorporadas en el iDRAC:

- Capa de sockets seguros (SSL)
- Solicitud de firma de certificado (CSR)
- Acceder a SSL mediante interfaz web
- Generación de una CSR
- Cómo cargar un certificado de servidor
- Cómo ver un certificado de servidor

Capa de sockets seguros (SSL)

El iDRAC6 incluye un servidor web que está configurado para usar el protocolo de seguridad SSL —que es el estándar de la industria— para transferir datos cifrados a través de una red. Como está cimentado en la tecnología de cifrado de claves privada y pública, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autenticada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Autenticarse ante un cliente habilitado con SSL
- Permitir que el cliente se autentique ante el servidor
- Permitir que ambos sistemas establezcan una conexión cifrada

El proceso de cifrado proporciona un alto nivel de protección de datos. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está generalmente disponible para los exploradores de Internet en Norteamérica.

De manera predeterminada, el servidor web del iDRAC6 tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del servidor web con un certificado firmado por una autoridad reconocida de certificados. Para iniciar el proceso de obtención de un certificado firmado, se puede usar la interfaz web del iDRAC6 para generar una solicitud de firma de certificado (CSR) con la información de la empresa. Usted podrá enviar entonces la CSR generada a una autoridad de certificados como VeriSign o Thawte.

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una CA para obtener un certificado de servidor seguro. Los certificados de servidor seguro hacen que los clientes del servidor confíen en la identidad del servidor al que se conectan y que negocien una sesión cifrada con el servidor.

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis confiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Una vez que la CA recibe una CSR, revisan y verifican la información que contiene la CSR. Si el solicitante cumple los estándares de seguridad de la CA, esta última emite un certificado firmado por medios digitales que identifica al solicitante de forma exclusiva para transacciones a través de redes y en Internet.

Después de que la autoridad de certificados apruebe la CSR y envíe el certificado, cargue el certificado en el firmware del iDRAC6. La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información contenida en el certificado.

Acceder a SSL mediante interfaz web

1. Haga clic en **Acceso Remoto**→ **Configuración.**
2. Haga clic en **SSL** para abrir la página **SSL**.

Use la página de **SSL** para realizar alguna de las siguientes acciones:

- Generar una solicitud de firma de certificado (CSR) para enviar a una CA. La información de la CSR se almacena en el firmware del iDRAC6.
- Cargar un certificado del servidor.
- Ver un certificado del servidor.

Tabla 4-11 describe las opciones anteriores de la página **SSL**.

Tabla 4-11. Opciones de página SSL

Campo	Descripción
Solicitud de firma de certificado (CSR)	Esta opción le permite generar una CSR para enviar a una CA para solicitar un certificado web seguro. **NOTA:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la CA acepte la CSR, la CSR que está en el firmware debe coincidir con el certificado que la CA devuelve.
Cargar certificado de servidor	Esta opción le permite cargar un certificado existente sobre el que su compañía tenga derechos y que utiliza para controlar el acceso al iDRAC6. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509, base 64. No acepta certificados codificados DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su iDRAC6
Ver el certificado de servidor	Esta opción le permite ver un certificado de servidor existente.

Generación de una solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. Antes de que el iDRAC pueda aceptar su CSR firmada, la CSR en el firmware debe coincidir con el certificado que la CA devuelve.

1. En la página **SSL**, seleccione **Generar solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**.
2. En la página **Generar solicitud de firma de certificado (CSR)**, introduzca un valor para cada atributo de la CSR. La Tabla 4-12 describe los atributos de la CSR.
3. Haga clic en **Generar** para crear la CSR y descargarla en su equipo local.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-13.

Tabla 4-12. Atributos para generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre de dominio del iDRAC, por ejemplo, **www.empresaxyz.com**). Son válidos los caracteres alfanuméricos, guiones, guiones bajos, espacios y puntos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad organizacional, como un departamento (por ejemplo, Tecnología informática). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo u otro carácter.
Nombre del estado	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Texas). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Escriba la dirección de correo electrónico de la empresa o cualquier dirección de correo electrónico asociada con la CSR. Este campo es opcional.

Tabla 4-13. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime los valores de **Generar solicitud de firma de certificado** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Generar solicitud de firma de certificado**.
Generar	Genera una CSR y luego pide al usuario que lo guarde en un directorio específico.
Volver al menú principal de SSL	Regresa al usuario a la página **SSL**.

Carga de un certificado de servidor

1. En la página de **SSL**, seleccione **Cargar certificado de servidor** y seleccione **Siguiente.**

   Aparecerá la página **Cargar certificado de servidor**.

2. En el campo **Ruta de acceso del archivo**, escriba la ruta de acceso del certificado en el campo **Valor** o haga clic en **Examinar** para desplazarse hacia el archivo del certificado.

NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

3. Haga clic en **Aplicar**.

4. Haga clic en el botón correspondiente de la página para continuar. Vea la Tabla 4-14.

Tabla 4-14. Botones de la página de carga de certificados

Botón	Descripción
Imprimir	Imprime la página **Carga de certificados**.
Volver al menú principal de SSL	Regresa a la página **Menú principal de SSL**.
Aplicar	Aplica el certificado al firmware del iDRAC6.

Cómo ver un certificado de servidor

1. En la página **SSL**, seleccione **Ver certificado del servidor** y haga clic en **Siguiente**.

   La página **Ver certificado del servidor** muestra el certificado de servidor que cargó al iDRAC.

   La Tabla 4-15 describe los campos y las descripciones asociadas que aparecen en la tabla **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-16.

Tabla 4-15. Información de certificados

Campo	Descripción
Número de serie	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el sujeto
Información del emisor	Atributos del certificado devueltos por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de vencimiento del certificado

Tabla 4-16. Botones de página de visualización de certificados del servidor

Botón	Descripción
Imprimir	Imprime los valores de **Ver certificado del servidor** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Ver certificado del servidor**.
Volver al menú principal de SSL	Vuelve a la página **SSL.**

Configuración y administración de certificados de Active Directory

La página le permite configurar y gestionar las configuraciones de Active Directory.

NOTA: Debe tener el permiso para **Configurar el iDRAC** para usar o configurar Active Directory.

NOTA: Antes de configurar o de usar la función de Active Directory, deberá asegurarse de que el servidor de Active Directory esté configurado para comunicarse con el iDRAC6.

NOTA: Para obtener información detallada sobre la configuración de Active Directory y cómo configurar Active Directory con un Esquema ampliado o un esquema estándar, consulte "Uso del iDRAC6 con Microsoft Active Directory".

Para acceder a la página **Configuración y administración de Active Directory**:

1. Haga clic en **Acceso Remoto**→ **Configuración**
2. Haga clic en **Active Directory** para abrir la página **Configuración y administración de Active Directory**.

   La Tabla 4-17 describe las opciones de la página **Configuración y administración de Active Directory**.
3. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-18.

Tabla 4-17. Opciones de la página Configuración y administración de Active Directory

Atributo	Descripción
Valores comunes	
Active Directory activado	Especifica si Active Directory está activado o desactivado.
Inicio de sesión único activado	Especifica si el inicio de sesión único está activado o desactivado. Si está activado, puede iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autenticación de usuario de dominio, como por ejemplo nombre de usuario y contraseña. Los valores posibles son **Sí** y **No**.
Selección de esquema	Especifica si se usa el esquema estándar o ampliado con Active Directory. **NOTA:** En esta versión, las funciones de autenticación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el esquema ampliado.
Nombre de dominio del usuario	Este valor sostiene hasta 40 entradas de dominios de usuarios. Si está configurada, la lista de nombres de dominios de usuarios aparecerá en la página de inicio de sesión en forma de menú desplegable para que el usuario elija una opción. Si no está configurada, los usuarios de Active Directory aún pueden iniciar sesión introduciendo el nombre de usuario en el formato nombre_de_usuario@nombre_de_dominio, nombre_de_dominio/nombre_de_usuario o nombre_de_dominio\nombre_de_usuario.
Expiración de tiempo	El tiempo en segundos de espera para que terminen las consultas a Active Directory. El valor predeterminado es 120 segundos.
Dirección del servidor del controlador de dominio 1-3 (FQDN o IP)	Especifica el nombre de dominio completo (FQDN) del controlador de dominio o la dirección IP. Es necesario configurar al menos una de las 3 direcciones. El iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. Si se selecciona el esquema ampliado, éstas son las direcciones de los controladores de dominio donde se encuentran el objeto dispositivo del iDRAC y los objetos de asociación. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.
Validación de certificados activada	El iDRAC utiliza el protocolo ligero de acceso a directorios (LDAP) a través de la capa de sockets seguros (SSL) mientras se conecta a Active Directory De manera predeterminada, el iDRAC utiliza el certificado de CA cargado en el iDRAC para validar el certificado del servidor de la capa de sockets seguros (SSL) de los controladores de dominio durante el protocolo de enlace SSL, lo que proporciona una fuerte seguridad. La validación de certificados se puede desactivar con fines de prueba o el administrador del sistema elige confiar en los controladores de dominio en el límite de seguridad sin validar sus certificados de la capa de sockets seguros (SSL). Esta opción especifica si la validación de certificados está activada o desactivada..
Certificado de CA de Active Directory	
Certificado	El certificado de la autoridad de certificados que firma el certificado del servidor de capa de sockets seguros (SSL) del controlador de dominio.
Configuración del esquema ampliado	**Nombre del iDRAC:** Especifica el nombre que identifica de forma única al iDRAC en Active Directory. De manera predeterminada, este valor es NULO. **Nombre de dominio del iDRAC**: El nombre de DNS (cadena) del dominio donde el objeto del iDRAC de Active Directory reside. De manera predeterminada, este valor es NULO. Estos valores sólo aparecerán si el iDRAC fue configurado para utilizarse con el esquema ampliado de Active Directory.
Configuración del esquema estándar	**Dirección del servidor del catálogo global 1-3 (FQDN o IP)**: Especifica el nombre de dominio completo (FQDN) o la dirección IP de los servidores del catálogo global. Es necesario configurar al menos una de las 3 direcciones. El iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. El servidor del catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. **Grupos de funciones** : especifica la lista de grupos de función asociados al iDRAC6. **Nombre de grupo:** especifica el nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC6. **Dominio de grupo**: indica el dominio del grupo. **Privilegio de grupo**: especifica el nivel de privilegios del grupo. Estos valores sólo aparecerán si el iDRAC fue configurado para utilizarse con el esquema estándar de Active Directory.

Tabla 4-18. Botones de la página Configuración y administración de Active Directory

Botón	Definición

Imprimir	Imprime los valores que se muestran en la página Configuración y administración de Active Directory.
Actualizar	Vuelve a cargar la página Configuración y administración de Active Directory.
Configurar Active Directory	Le permite configurar Active Directory. Para obtener información detallada de configuración, consulte "Uso del iDRAC6 con Microsoft Active Directory".
Probar configuración	Permite que usted verifique la configuración de Active Directory con las configuraciones especificadas. Consulte "Uso del iDRAC6 con Microsoft Active Directory" para obtener detalles sobre el uso de la opción **Probar configuración**.

Configuración de los servicios del iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

1. Haga clic en **Acceso Remoto**→ **Configuración.** Luego, haga clic en la lengüeta **Servicios** para mostrar la página de configuración **Servicios.**
2. Configure los servicios siguientes según sea necesario:
   - Configuración local: consulte la Tabla 4-19
   - Servidor web: consulte la Tabla 4-20 para ver la configuración del servidor web
   - SSH: consulte la Tabla 4-21 para ver la configuración de SSH
   - Telnet: consulte la Tabla 4-22 para ver la configuración de Telnet
   - RACADM remoto: consulte la Tabla 4-23 para ver la configuración de RACADM remoto
   - Agente SNMP: consulte la Tabla 4-24 para ver la configuración de SNMP
   - Agente de recuperación automática del sistema (ASR): consulte la Tabla 4-25 para ver la configuración del agente ASR.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-26.

Tabla 4-19. Configuración local

Valor	Descripción
Desactivar la configuración local del iDRAC por medio de la ROM de opción	Desactiva la configuración local del iDRAC por medio de la ROM de opción La ROM de opción se encuentra en el BIOS y proporciona un motor de interfaz del usuario que permite la configuración del iDRAC y BMC. La ROM de opción le pedirá que introduzca el módulo de configuración presionando <Ctrl+E>.
Desactivar la configuración local del iDRAC por medio de RACADM	Desactiva la configuración local del iDRAC por medio de RACADM local.

Tabla 4-20. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor web del iDRAC6. Cuando está seleccionada, la casilla indica que el servidor web está activado. El valor predeterminado es **activado**.
Máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Este campo no se puede editar. La cantidad máxima de sesiones simultáneas es cinco.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al valor de **Máx. de sesiones**. Este campo no se puede editar.
Expiración de tiempo	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cierra cuando se alcanza la expiración de tiempo. Los cambios a la configuración de expiración de tiempo actúan de inmediato y finalizan la sesión de interfaz web actual. También se restablecerá el servidor web. Espere unos minutos antes de abrir una nueva sesión de interfaz web. El rango de expiración de tiempo es de 60 a 10800 segundos El valor predeterminado es de 1800 segundos.
Número de puerto HTTP	El puerto en el que el iDRAC6 espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto HTTPS	El puerto en el que el iDRAC6 espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 4-21. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando está seleccionada, la casilla indica que SSH está activado.
Expiración de tiempo	La expiración de tiempo en inactividad de Secure Shell, expresado en segundos. El rango de expiración de tiempo es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de expiración de tiempo. El valor predeterminado es **300**.

Número de puerto	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 4-22. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado.
Expiración de tiempo	La expiración de tiempo de inactividad del Telnet, en segundos. El rango de expiración de tiempo es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de expiración de tiempo. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 4-23. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Cuando se selecciona, la RACADM remota está activada.
Sesiones activas	El número de sesiones actuales en el sistema.

Tabla 4-24. Configuración de SNMP

Valor	Descripción
Activado	Activa/desactiva SNMP. Cuando se selecciona, SNMP está activado.
Nombre de comunidad SNMP	Activa/desactiva el nombre de comunidad SNMP Cuando se selecciona, el nombre de comunidad SNMP está activado. El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 4-25. Configuración del agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automática del sistema. Cuando se selecciona, el agente de recuperación automática del sistema está activado.

Tabla 4-26. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

Actualización del firmware del iDRAC6/imagen de recuperación de los servicios del sistema

NOTA: Si el firmware del iDRAC6 se daña, como puede suceder cuando el progreso de la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio de la interfaz web del iDRAC6.

NOTA: De manera predeterminada, la actualización del firmware retendrá la configuración actual del iDRAC6. Durante el proceso de actualización, usted tiene la opción de restablecer los valores predeterminados de fábrica para la configuración del iDRAC6. Si establece la configuración a valores predeterminados de fábrica, debe configurar la red utilizando la utilidad de configuración del iDRAC6.

1. Abra la interfaz web del iDRAC6 e inicie sesión en el sistema remoto.
2. Haga clic en **Acceso remoto** y luego en la lengüeta **Actualizar**.
3. En la página **Cargar/Revertir (Paso 1 de 3)** haga clic en **Examinar** o escriba la ruta de acceso a la imagen del firmware que descargó de **support.dell.com** o la imagen de recuperación de servicios del sistema.

   NOTA: Si ejecuta Firefox, el cursor de texto no aparecerá en el campo **Imagen de firmware**.

   Por ejemplo:

   `C:\Updates\V1.0\<nombre_de_imagen>`.

O bien:

```
\\192.168.1.10\Updates\V1.0\<nombre_de_imagen>
```

El nombre predeterminado de la imagen de firmware es **firmimg.d6**.

4. Haga clic en **Cargar**.

   El archivo se cargará en el iDRAC6. Este proceso puede tardar varios minutos en completarse.

   El siguiente mensaje se mostrará hasta que el proceso se complete:

   ```
   File upload in progress... (Carga de archivo en progreso...)
   ```

5. En la página **Estado (página 2 de 3)**, verá los resultados de la validación realizada sobre el archivo de imagen que usted cargó.

   - Si la imagen ha sido cargada exitosamente y aprobó todas las verificaciones, el nombre del archivo de imagen se mostrará. Si una imagen de firmware fue cargada, las versiones actuales y las nuevas de firmware se mostrarán.

     O bien:

   - Si la imagen no ha sido cargada exitosamente y no aprobó todas las verificaciones, un mensaje de error apropiado aparecerá y la actualización regresará a la página **Cargar/Revertir (Paso 1 de 3).** Puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

- En el caso de una imagen de firmware, la función **Conservar configuración** le proporciona la opción de preservar o eliminar la configuración del iDRAC6 existente. Esta opción está seleccionada de forma predeterminada.

  NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está activada. Usted no podrá iniciar sesión en la interfaz web del iDRAC6. Debe reconfigurar los valores de la LAN por medio de la utilidad de configuración del iDRAC6 durante la POST (Power-On Self-Test [autoprueba de encendido]) del BIOS.

7. Haga clic en **Actualizar** para iniciar el proceso de actualización.

8. En la página **Actualización (Paso 3 de 3)**, verá el estado de la actualización. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.

   NOTA: Mientras se encuentra en modo actualización, el proceso de actualización continuará en segundo plano incluso si su navegador ya no se encuentra en este página.

   Si la actualización del firmware es exitosa, el iDRAC se restablecerá automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador. Se muestra un mensaje de error si se detecta algún error.

   Si la actualización del sistema de recuperación de servicios se completa/falla, un mensaje de estado apropiado aparecerá.

Reversión del firmware del iDRAC6

iDRAC6 es capaz de mantener dos imágenes de firmware simultáneas. Puede optar por iniciar desde la imagen de firmware de su elección o revertir el firmware a dicha imagen.

1. Abra la interfaz web del iDRAC6 e inicie sesión en el sistema remoto.

   Haga clic en **Sistema**→ **Acceso remoto** y luego en la lengüeta **Actualizar**.

2. En la página **Cargar/Revertir (Paso 1 de 3)**, haga clic en **Revertir**. Las versiones de firmware actuales y anteriores se muestran en la página **Estado (Paso 2 de 3).**

   Conservar configuración le proporciona la opción para conservar o limpiar la configuración del iDRAC6 existente. Esta opción está seleccionada de forma predeterminada.

   NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está activada. Usted no podrá iniciar sesión en la interfaz web del iDRAC6. Deberá reconfigurar los valores de la LAN por medio de la utilidad de configuración del iDRAC6 durante la POST (Power-On Self-Test [autoprueba de encendido]) del BIOS o el comando racadm (localmente disponible en el servidor).

3. Haga clic en **Actualizar** para iniciar el proceso de actualización del firmware.

   En la página **Actualización** (Paso 3 de 3), se mostrará el estado de la operación de reversión. El progreso aparece medido en porcentajes en la columna **Progreso**.

   NOTA: Mientras se encuentra en modo actualización, el proceso de actualización continuará en segundo plano incluso si su navegador ya no se encuentra en este página.

   Si la actualización del firmware es exitosa, el iDRAC se restablecerá automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador. Se muestra un mensaje de error si se detecta algún error.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración avanzada del iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección ofrece información sobre la configuración avanzada del iDRAC6. Su lectura se recomienda especialmente para los usuarios con conocimientos avanzados sobre la administración de sistemas que deseen personalizar el entorno del iDRAC6 de acuerdo con sus necesidades específicas.

Antes de comenzar

Usted debe haber terminado la instalación y configuración básica del hardware y software del iDRAC6. Consulte "Instalación básica de un iDRAC6" para obtener más información.

Configuración del iDRAC6 para visualizar la salida de la comunicación serial de forma remota a través de SSH/Telnet

Puede configurar el iDRAC6 para redireccionamiento remoto de la consola de comunicación serial siguiendo estos pasos:

Primero, configure el BIOS para permitir el redireccionamiento de la consola de comunicación serial:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   ```
   <F2> = System Setup (Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure las opciones en pantalla de la **Comunicación serie** como se indica a continuación:

   ```
   serial communication....On with serial redirection via com2 (Comunicación serial....Activada con redireccionamiento serial a través de com2)
   ```

   NOTA: Puede configurar la comunicación serial en **Activada con redireccionamiento serial a través de com1** siempre que el campo de dirección del puerto serial, dispositivo serial2, esté configurado en com1, también.

   ```
   serial port address....Serial device1 = com1, serial device2 = com2 (Dirección del puerto serial....Dispositivo serial1 = com1, dispositivo serial2 = com2)

   external serial connector....Serial device 1 (Conector serial externo....dispositivo serial1)

   failsafe baud rate....115200 (velocidad en baudios segura....115200)

   remote terminal type....vt100/vt220 (tipo de terminal remota....vt100/vt220)

   redirection after boot....Enabled (redireccionamiento después del inicio....Activado)
   ```

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Configuración de los valores del iDRAC6 para activar SSH/Telnet

Luego, configure los valores del iDRAC6 para activar SSH/Telnet, que puede realizar a través de RACADM o la interfaz web del iDRAC6.

Para cambiar la configuración del iDRAC6 para activar SSH/Telnet usando RACADM, ejecute los comandos siguientes:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

También puede ejecutar los comandos RACADM remotamente; consulte "Uso de RACADM de manera remota".

Para cambiar la configuración del iDRAC6 para activar SSH/Telnet usando la interfaz web del iDRAC6, siga estos pasos:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Servicios**.
3. Seleccione **Activar** en la sección **SSH** o **Telnet**.
4. Haga clic en **Aplicar cambios**.

El paso siguiente es conectarse al iDRAC6 usando Telnet o SSH.

Inicio de una consola de texto en Telnet o SSH

Después de haber iniciado sesión en el iDRAC6 a través del software de terminal de la estación de administración con Telnet o SSH, usted puede desviar la consola de texto del sistema administrado por medio de **console com2**, que es un comando de Telnet/SSH. Sólo se admite un cliente de **console com2** a la vez.

Para conectarse a la consola de texto del sistema administrado, abra una petición de comandos del iDRAC6 (a través de una sesión de Telnet o SSH) y escriba:

```
console com2
```

El comando `console -h com2` muestra el contenido del búfer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serie.

El tamaño predeterminado (y máximo) del búfer de historial es de 8192 caracteres. Puede asignar un número menor a este valor con el comando:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <número>
```

Para configurar Linux para direccionamiento de consola durante el inicio, consulte "Configuración de Linux para la redirección de la consola serie durante el inicio".

Uso de una consola de Telnet

Ejecutar Telnet usando Microsoft® Windows® XP o Windows 2003

Si la estación de administración ejecuta Windows XP o Windows 2003, pueden presentarse problemas de caracteres en una sesión Telnet del iDRAC6. El problema puede consistir en un inicio de sesión bloqueado en el que la tecla <Entrar> no responde y no aparece la solicitud para introducir la contraseña.

Para resolver este problema, descargue la revisión (hotfix) 824810 del sitio web de asistencia de Microsoft en **support.microsoft.com**. Consulte el artículo 824810 de Microsoft Knowledge Base para obtener más información.

Ejecución de Telnet con Windows 2000

Si la estación de administración ejecuta Windows 2000, no se podrá acceder a la configuración del BIOS al presionar la tecla <F2>. Para resolver este problema, use el cliente Telnet que se incluye en la descarga gratuita recomendada de los servicios de Windows para UNIX® 3.5 de Microsoft. Vaya a **www.microsoft.com/downloads/** y busque "*Windows Services for UNIX 3.5*." (Servicios de Windows para UNIX 3.5).

Activación de Telnet de Microsoft para redirección de consola Telnet

NOTA: Es posible que algunos clientes Telnet en los sistemas operativos Microsoft no muestren correctamente la pantalla de configuración del BIOS cuando la redirección de la consola de BIOS está configurada para la emulación de VT100/VT220. Si se presenta este problema, cambie la redirección de la consola de BIOS al modo ANSI para actualizar la ventana. Para realizar este procedimiento en el menú de configuración del BIOS, seleccione **Redirección de consola** → **Tipo de terminal remota** → **ANSI**.

NOTA: Cuando configure la ventana de emulación de cliente VT100, configure la ventana o aplicación que está mostrando la consola redirigida en 25 filas x 80 columnas, a fin de garantizar que el texto se muestre correctamente. De lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

1. Active **Telnet** en **Servicios de componentes de Windows**.
2. Conéctese al iDRAC6 en la estación de administración.

   Abra una petición de comandos, escriba lo siguiente y presione <Entrar>:

telnet <*dirección IP*>:<*número de puerto*>

donde *dirección IP* es la dirección IP del iDRAC6 y el *número de puerto* es el número de puerto de Telnet (si se está usando un puerto nuevo).

Configuración de la tecla de retroceso para la sesión de Telnet

El uso de la tecla <Retroceso> puede producir resultados inesperados, según el cliente de Telnet. Por ejemplo, la sesión puede mostrar el eco ^h. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux se pueden configurar para usar la tecla <Retroceso>.

Para configurar los clientes Telnet de Microsoft para que utilicen la tecla <Retroceso>:

1. Abra una ventana de símbolo de sistema (si es necesario).
2. Si no está ejecutando una sesión de Telnet, escriba:

   ```
   telnet
   ```

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En la petición, escriba:

   ```
   set bsasdel
   ```

   Aparece el mensaje siguiente:

   ```
   Backspace will be sent as delete. (El retroceso se procesará como eliminación.)
   ```

Para configurar una sesión de Telnet de Linux a fin de que utilice la tecla <Retroceso>:

1. Abra una petición de comandos y escriba:

   ```
   stty erase ^h
   ```
2. En la petición, escriba:

   ```
   telnet
   ```

Uso de Secure Shell (SSH)

Es crucial que los dispositivos del sistema y la administración de dispositivos estén seguros. Los dispositivos incorporados y conectados son el centro medular de muchos procesos comerciales. Si estos dispositivos son vulnerables, la empresa puede estar en riesgo, lo que requiere de nuevas exigencias de seguridad al software de administración de dispositivos mediante interfaz de línea de comandos (CLI).

Secure Shell (SSH) es una sesión de línea de comandos que incluye las mismas capacidades que una sesión de Telnet, pero con mayor seguridad. El iDRAC6 admite la versión 2 de SSH con autenticación por contraseña. SSH está activo en el iDRAC6 cuando instala o actualiza el firmware del iDRAC6.

Se puede usar PuTTY u OpenSSH en la estación de administración para conectarse al iDRAC6 del sistema administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente Secure Shell envía un mensaje de error. El texto del mensaje depende del cliente y no es controlado por el iDRAC6.

NOTA: OpenSSH se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. La ejecución de OpenSSH en la petición de comandos de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

Sólo se admiten cuatro sesiones SSH a la vez. La expiración de tiempo de la sesión la controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se describe en "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

Para activar SSH en el iDRAC6, escriba:

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Para cambiar el puerto SSH, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>
```

Para obtener más información sobre las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

La implementación de SSH del iDRAC6 admite varios esquemas de criptografía, según se muestra en Tabla 5-1.

Tabla 5-1. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS 512:1024 bits (aleatorios) según la especificación NIST

Criptografía simétrica	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Integridad de mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autenticación	• Contraseña

NOTA: No se admite SSHv1.

Configuración de Linux para la redirección de la consola serie durante el inicio

Los pasos a continuación son específicos para GRand Unified Bootloader (GRUB) de Linux. Será necesario hacer cambios similares si se utiliza otro cargador de inicio.

NOTA: Cuando configure la ventana de emulación de cliente VT100, configure la ventana o aplicación que esté mostrando la consola redirigida en 25 filas x 80 columnas a fin de garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo **/etc/grub.conf** como se indica a continuación:

1. Localice las secciones de configuración general dentro del archivo y agregue las siguientes dos líneas:

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```

2. Agregue dos opciones a la línea de núcleo:

   ```
   kernel ..... console=ttyS1,115200n8r console=tty1
   ```

3. Si el archivo **/etc/grub.conf** contiene una directiva splashimage, inserte un carácter de comentario al inicio de la línea para anularla.

La Tabla 5-2 contiene un ejemplo del archivo **/etc/grub.conf** que muestra los cambios que se describen en este procedimiento.

Tabla 5-2. Archivo de ejemplo: /etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Cuando modifique el archivo **/etc/grub.conf**, aplique las siguientes directrices:

1. Desactive la interfaz gráfica de GRUB y utilice la interfaz de texto; de lo contrario, la pantalla de GRUB no aparecerá en la redirección de consola del RAC. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con splashimage.

2. Para activar varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión en serie del RAC, agregue la siguiente línea a todas las opciones:

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   La Tabla 5-2 muestra la cadena `console=ttyS1,57600` ya agregada a la primera opción solamente.

Activación del inicio de sesión en la consola después de inicio

Modifique el archivo **/etc/inittab** según se indica a continuación:

Agregue una nueva línea para configurar agetty en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

La Tabla 5-3 muestra un archivo de ejemplo con la nueva línea.

Tabla 5-3. Archivo de ejemplo: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifique el archivo **/etc/securetty** según se indica a continuación:

Agregue una nueva línea con el nombre del tty serie para COM2:

```
ttyS1
```

La Tabla 5-4 muestra un archivo de ejemplo con la nueva línea.

Tabla 5-4. Archivo de ejemplo: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Configuración del iDRAC6 para conexión serial

Puede usar cualquiera de las interfaces siguientes para conectarse al iDRAC6 a través de una conexión serial:

- Interfaz de línea de comandos del iDRAC6
- Modo básico de conexión directa
- Modo de terminal de conexión directa

Para configurar su sistema para usar cualquiera de estas interfaces, realice los pasos siguientes.

Configure el **BIOS** para activar conexiones seriales:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   `<F2> = Programa de configuración del sistema`

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure la pantalla **Comunicación serie** como se indica a continuación:

   Conector serie externo....dispositivo de acceso remoto

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Luego, conecte el cable DB-9 o de módem nulo de la estación de administración al servidor administrado en nodo. Consulte "Conexión del cable de módem nulo o DB-9 para la consola serial".

Posteriormente, asegúrese de que el software emulador de terminal de administración esté configurado para conexiones seriales. Consulte "Configuración del software de emulación de terminal de la estación de administración".

Luego, configure los valores del iDRAC6 para activar conexiones seriales, que puede realizar a través de RACADM o la interfaz web del iDRAC6.

Para cambiar la configuración del iDRAC6 para activar conexiones seriales usando RACADM, ejecute el comando siguiente:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Para cambiar la configuración del iDRAC6 para activar conexiones seriales usando la interfaz web del iDRAC6, siga estos pasos:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Serie**.
3. Seleccione **Activado** en la sección **RAC Serial**.
4. Haga clic en **Aplicar cambios**.

Cuando ha establecido una conexión serial con la configuración anterior, deberá ver una petición de contraseña. Introduzca el nombre de usuario y la contraseña del iDRAC6 (los valores predeterminados son `root` y `calvin`, respectivamente).

Desde esta interfaz, puede ejecutar varias funciones como RACADM. Por ejemplo, para imprimir el registro de eventos del sistema, introduzca el siguiente comando RACADM:

```
racadm getsel
```

Configuración del iDRAC para el modo básico de conexión directa y el modo de terminal de conexión directa

Usando RACADM, ejecute el siguiente programa para desactivar la interfaz de línea de comandos del iDRAC6:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

Posteriormente, ejecute el siguiente comando RACADM para activar el modo básico de conexión directa:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 1
```

O, ejecute el siguiente comando RACADM para activar el modo de terminal de conexión directa:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode 0
```

Puede realizar las mismas acciones usando la interfaz web del iDRAC6:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Serie**.
3. Deseleccione **Activado** en la sección **RAC Serial**.

   Para el modo básico de conexión directa:

   En la sección **IPMI Serial** cambie la opción del menú desplegable **Configuración del modo de conexión** a **Modo básico de conexión directa**.

   Para el modo de terminal de conexión directa:

   En la sección **IPMI Serial** cambie la opción del menú desplegable **Configuración del modo de conexión** a **Modo de terminal de conexión directa**.
4. Haga clic en **Aplicar cambios**. Para obtener más información sobre los modos básico y de terminal de conexión directa, consulte "Configuración de los modos serie y terminal".

El modo básico de conexión directa le permitirá usar herramientas como ipmish directamente a través de la conexión serial. Por ejemplo, para imprimir el registro de eventos del sistema usando ipmish a través del modo básico de IPMI, ejecute el comando siguiente:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

El modo de terminal de conexión directa le permitirá enviar comandos ASCII al iDRAC6. Por ejemplo, para encender/apagar el servidor a través del modo de terminal de conexión directa:

1. Conéctese al iDRAC6 por medio del software de emulación de terminal
2. Escriba el comando siguiente para iniciar sesión:

   ```
   [SYS PWD -U root calvin]
   ```

   Verá la respuesta siguiente:

   ```
   [SYS]
   ```

   ```
   [OK]
   ```
3. Escriba el comando siguiente para verificar un inicio de sesión exitoso:

   ```
   [SYS TMODE]
   ```

   Verá la respuesta siguiente:

   ```
   [OK TMODE]
   ```
4. Para apagar el servidor (el servidor se apagará inmediatamente), escriba el comando siguiente:

   ```
   [SYS POWER OFF]
   ```
5. Para encender el servidor (el servidor encenderá inmediatamente):

   ```
   [SYS POWER ON]
   ```

Cambio entre el modo de comunicación de interfaz serie de RAC y la redirección de consola serie

El iDRAC6 admite el uso de secuencias de la tecla Esc para alternar entre la comunicación de interfaz serie de RAC y la redirección de consola serie.

Para configurar el sistema de forma tal que permita este procedimiento, siga estas instrucciones:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   ```
   <F2> = System Setup (Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure la pantalla **Comunicación serie** como se indica a continuación:

   comunicación serial -- Activada con redireccionamiento serial a través de com2

   NOTA: Puede configurar el campo de **comunicación serial** a **Activado con redireccionamiento a través de com1** siempre que **dispositivo serial2** en el campo de la **dirección del puerto serial** también esté configurado en com1.

   Dirección del puerto serial -- Dispositivo serial1 = com1, dispositivo serial2 = com2

   Conector serial externo -- dispositivo serial2

   velocidad en baudios segura....115200

   tipo de terminal remota ...vt100/vt220

   redireccionamiento después del inicio ... Activado

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Conecte el cable de módem nulo entre el conector serie externo del sistema administrado y el puerto serie de la estación de administración.

Utilice un programa de emulación de terminal (HyperTerminal o Teraterm) en la estación de administración y, de acuerdo con la etapa del proceso de inicio del servidor administrado, podrá ver las pantallas POST (Power-On Self-Test [autoprueba de encendido]) o del sistema operativo. Este procedimiento toma como base la configuración SAC para Windows y pantallas de modo de texto para Linux. Defina los siguientes valores de configuración de terminal de la estación de administración: velocidad en baudios: 115200; datos: 8 bits, paridad: ninguna, detención: 1 bit de parada y control de flujo: ninguno.

Para pasar al modo de comunicación de interfaz serie de RAC desde el modo de redirección de consola serie, utilice la siguiente secuencia de teclas:

```
<Esc> +<Mayús> <9>
```

Esta secuencia activa la petición "Inicio de sesión del iDRAC" (si el RAC está en el modo "RAC serie") o bien el modo "Conexión en serie" en el que pueden emitirse comandos de terminal (si el RAC se encuentra en "Modo de terminal de conexión directa en serie de IPMI").

Para cambiar al modo de redirección de consola serie desde el modo de comunicación de interfaz serie de RAC, use la siguiente secuencia de teclas:

```
<Esc> +<Mayús> <q>
```

Conexión del cable de módem nulo o DB-9 para la consola serial

Para acceder al sistema administrado con una consola de texto serie, conecte un cable de módem nulo DB-9 al puerto COM del sistema administrado. Con objeto de que la conexión funcione con el cable de módem nulo, se deberán realizar las configuraciones correspondientes de comunicaciones seriales en la configuración de CMOS. No todos los cables DB-9 tienen la asignación de patas/señales necesarias para esta conexión. El cable DB-9 de esta conexión debe cumplir las especificaciones que se muestran en la Tabla 5-5.

NOTA: El cable DB-9 también se puede usar para la redirección de consola de texto de BIOS.

Tabla 5-5. Asignación de patas necesaria para el cable de módem nulo DB-9

Nombre de señal	Pata DB-9 (pata de servidor)	Pata DB-9 (pata de estación de trabajo)
FG (protección de tierra)	–	–
TD (transmisión de datos)	3	2
RD (recepción de datos)	2	3
RTS (solicitud de envío)	7	8
CTS (listo para envío)	8	7

SG (señal de tierra)	5	5
DSR (conjunto de datos listo)	6	4
CD (detección de transportador)	1	4
DTR (terminal de datos listo)	4	1 y 6

Configuración del software de emulación de terminal de la estación de administración

El iDRAC6 admite una consola de texto Telnet o serie de una estación de administración que ejecute uno de los siguientes tipos de software de emulación de terminal:

- Linux Minicom en Xterm
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve
- Linux Telnet en Xterm
- Microsoft Telnet

Realice los pasos en los apartados siguientes para configurar el tipo del software de terminal. Si está usando Microsoft Telnet, no se requiere la configuración.

Configuración de Linux Minicom para la emulación de consola serie

Minicom es la utilidad de acceso a puerto serie de Linux. Los pasos siguientes son válidos para configurar Minicom versión 2.0. Otras versiones de Minicom pueden diferenciarse ligeramente, pero requieren los mismos valores básicos. Utilice la información en "Valores de Minicom necesarios para la emulación de consola serie" para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0 para emulación de la consola serie

NOTA: Para garantizar que el texto se muestre correctamente, Dell recomienda que se utilice una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece el sistema Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en la petición de comandos.
2. En la ventana de Xterm, lleve la flecha del ratón a la esquina inferior derecha de la ventana y cambie el tamaño de la ventana a 80 x 25.
3. Si no tiene un archivo de configuración de Minicom, vaya al siguiente paso.

   Si tiene un archivo de configuración de Minicom, escriba `minicom <nombre del archivo de configuración de Minicom>` y luego vaya al paso 17.
4. En la petición de comandos de Xterm, escriba `minicom -s`.
5. Seleccione **Configuración del puerto serie** y presione <Entrar>.
6. Presione <a> y seleccione el dispositivo serie correspondiente (por ejemplo, **/dev/ttyS0**).
7. Presione <e> y establezca la opción **Bps/Par/Bits** en **57600 8N1**.
8. Presione <f> y establezca **Control de flujo de hardware** en **Sí** y **Control de flujo de software** en **No**.
9. Para salir del menú **Configuración del puerto serie**, presione <Entrar>.
10. Seleccione **Módem y marcación** y presione <Entrar>.
11. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco.
12. Presione <Entrar> para guardar cada uno de los valores en blanco.
13. Cuando se hayan borrado todos los campos especificados, presione <Entrar> para salir del menú **Configuración de parámetros y marcación de módem**.
14. Seleccione **Guardar configuración como nombre_de_config** y presione <Entrar>.
15. Seleccione **Salir de Minicom** y presione <Entrar>.

16. En la petición del shell de comandos, escriba `minicom <nombre del archivo de configuración de Minicom>`.

17. Para ampliar la ventana de Minicom a 80 x 25, arrastre la esquina de la misma.

18. Presione <Ctrl+a>, <z>, <x> para salir de Minicom.

NOTA: Si utiliza Minicom para la redirección de consola de texto serie para configurar el BIOS del sistema administrado, se recomienda activar el color en Minicom. Para activar el color, escriba el comando siguiente: `minicom -c on`

Asegúrese de que la ventana Minicom muestre una petición de comando. Cuando la petición de comandos aparezca, la conexión se habrá establecido satisfactoriamente y estará listo para conectarse a la consola del sistema administrado por medio del comando serie **connect**.

Valores de Minicom necesarios para la emulación de consola serie

Utilice la Tabla 5-6 para configurar cualquier versión de Minicom.

Tabla 5-6. Valores de Minicom para emulación de consola serie

Descripción del valor	Valor necesario
Bps/Par/Bits	57600 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Marcación de módem y configuración de parámetros	Borre los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco
Tamaño de ventana	80 x 25 (para cambiar el tamaño, arrastre la esquina de la ventana)

Configuración de HyperTerminal para la redirección de consola serie

HyperTerminal es la utilidad de acceso de puerto serie de Microsoft Windows. Para establecer el tamaño de la pantalla de consola correctamente, utilice HyperTerminal Private Edition versión 6.3 de Hilgraeve.

PRECAUCIÓN: Todas las versiones del sistema operativo Microsoft Windows incluyen el software de emulación de terminal HyperTerminal de Hilgraeve. Sin embargo, la versión incluida no proporciona numerosas funciones necesarias durante la redirección de consola. En su lugar, puede utilizar cualquier software de emulación de terminal que admita el modo de emulación VT100/VT220 o ANSI. Un ejemplo de un emulador de terminal VT100/VT220 o ANSI completo que admite la redirección de consola en el sistema es HyperTerminal Private Edition 6.3 de Hilgraeve. Además, el uso de la ventana de línea de comandos para ejecutar la redirección de consola serie Telnet puede dar lugar a la aparición de caracteres inservibles.

Para configurar HyperTerminal para la redirección de consola serie:

1. Inicie el programa HyperTerminal.

2. Escriba un nombre para la nueva conexión y haga clic en **Aceptar**.

3. Junto a **Conectar usando:**, seleccione el puerto COM en la estación de administración (por ejemplo, COM2) al que ha conectado el cable de módem nulo DB-9 y haga clic en **Aceptar**.

4. Configure los valores del puerto COM según se muestra en la Tabla 5-7.

5. Haga clic en **Aceptar**.

6. Haga clic en **Archivo** → **Propiedades** y después haga clic en la lengüeta **Configuración**.

7. Defina la **Id. de la terminal de Telnet:** como **ANSI**.

8. Haga clic en **Configuración de terminal** y establezca **Filas de pantalla** en **26**.

9. Establezca **Columnas** en **80** y haga clic en **Aceptar**.

Tabla 5-7. Configuración del puerto COM de la estación de administración

Descripción del valor	Valor necesario
Bits por segundo	57600
Bits de datos	8

Paridad	Ninguno
Bits de parada	1
Control de flujo	Hardware

Configuración de los modos serie y terminal

Configuración de la conexión serie de IPMI e iDRAC6

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Serie**.
3. Configure los valores de conexión serie de IPMI.

   Consulte la Tabla 5-8 para ver una descripción de los valores de la conexión serie de IPMI.
4. Configure los valores de conexión serie del iDRAC6.

   Consulte la Tabla 5-9 para ver una descripción de los valores de la conexión serie del iDRAC6.
5. Haga clic en **Aplicar cambios**.
6. Haga clic en el botón adecuado de la página **Configuración serie** para continuar. Consulte la Tabla 5-10 para ver una descripción de los valores de la página de configuración de la conexión serie.

Tabla 5-8. Configuración de la conexión serie de IPMI

Valor	Descripción
Configuración del modo de conexión	• Modo básico de conexión directa: Modo básico de conexión serie de IPMI • Modo de terminal de conexión directa: Modo de terminal de conexión serie de IPMI
Velocidad en baudios	• Establece la velocidad de los datos. Seleccione **9600 bps**, **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.
Control de flujo	• Ninguno: Control de flujo de hardware apagado • RTS/CTS: Control de flujo de hardware encendido
Límite del nivel de privilegios del canal	• Administrador • Operador • Usuario

Tabla 5-9. Valores de configuración del iDRAC6

Valor	Descripción
Activado	Activa o desactiva la consola serie del iDRAC6. Seleccionada=activada; deseleccionada=desactivada
Expiración de tiempo	La cantidad máxima de segundos de inactividad de la línea antes de que se desconecte. El rango es de 60 a 1920 segundos. El valor predeterminado es de 300 segundos. Utilice 0 segundos para desactivar la función de expiración de tiempo.
Redirección activada	Activa o desactiva la redirección de consola. Seleccionada=activada; deseleccionada=desactivada
Velocidad en baudios	La velocidad de los datos en el puerto serie externo. Los valores son **9600 bps**, **19,2 kbps**, **57,6 kbps** y **115,2 kbps**. El valor predeterminado es de **57,6 kbps**.
Tecla Escape	Especifica la tecla <Esc>. El valor predeterminado son los caracteres ^\.
Tamaño del búfer de historial	El tamaño del búfer de historial de la conexión serie, que guarda los últimos caracteres que se escribieron en la consola. El valor máximo y predeterminado es 8192 caracteres.
Comando de inicio de sesión	La línea de comando del iDRAC6 que se ejecutará ante un inicio de sesión válido.

Tabla 5-10. Valores de la página de configuración de la conexión serie

Botón	Descripción
Imprimir	Imprime la página **Configuración de la conexión serie**.

Actualizar	Actualiza la página **Configuración de la conexión serie**.
Aplicar cambios	Aplica los cambios de la conexión serie del iDRAC6 e IPMI.
Configuración del modo de terminal	Abre la página **Configuración del modo de terminal**.

Configuración del modo de terminal

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Serie**.
3. En la página **Serie**, haga clic en **Configuración del modo de terminal**.
4. Defina la configuración del modo de terminal.

   Consulte la Tabla 5-11 para ver una descripción de la configuración del modo de terminal.
5. Haga clic en **Aplicar cambios**.
6. Haga clic en el botón correspondiente de la página **Configuración del modo de terminal** para continuar. Consulte la Tabla 5-12 para ver una descripción de los botones de la página de configuración del modo de terminal.

Tabla 5-11. Configuración del modo de terminal

Valor	Descripción
Edición de línea	Activa o desactiva la edición de línea.
Control de eliminación	Seleccione una de las siguientes opciones: • **El iDRAC6 genera un carácter <retroceso><espacio><retroceso> cuando se recibe <retroceso> o <supr>**. • **El iDRAC6 genera un carácter <supr> cuando se recibe <retroceso> o <supr>**.
Control del eco	Activa o desactiva el eco.
Control del protocolo de enlace	Activa o desactiva el protocolo de enlace.
Nueva secuencia de línea	Seleccione **Ninguno**, **<CR-LF>**, **<NULO>**, **<CR>**, **<LF-CR>** o **<LF>**.
Introducir una nueva secuencia de línea	Seleccione **<CR>** o **<NULO>**.

Tabla 5-12. Botones de la página de configuración del modo de terminal

Botón	Descripción
Imprimir	Imprime la página **Configuración del modo de terminal**.
Actualizar	Actualiza la página **Configuración del modo de terminal**.
Regresar a Configuración del puerto serie	Regresa a la página **Configuración del puerto serie**.
Aplicar cambios	Aplica los cambios de la configuración del modo de terminal.

Configuración de los valores de red del iDRAC6

PRECAUCIÓN: Si cambia la configuración de red del iDRAC6, podría provocar que su conexión de red actual se desconecte.

Configure los valores de red del iDRAC6 con una de las herramientas siguientes:

- Interfaz web: consulte "Configuración de la tarjeta de interfaz de red del iDRAC6"
- Interfaz de línea de comandos de RACADM: consulte "cfgLanNetworking"
- Utilidad de configuración del iDRAC6: consulte "Configuración de su sistema para usar el iDRAC6"

NOTA: Si va a instalar el iDRAC6 en un entorno de Linux, consulte "Instalación de RACADM".

Acceso al iDRAC6 a través de una red

Después de configurar el iDRAC6, usted puede acceder de manera remota el sistema administrado por medio de una de las interfaces siguientes:

- Interfaz web
- RACADM
- Consola Telnet
- SSH
- IPMI

La Tabla 5-13 describe cada interfaz del iDRAC6.

Tabla 5-13. Interfaces del iDRAC6

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto al iDRAC6 por medio de una interfaz gráfica para el usuario. La interfaz web está integrada en el firmware del iDRAC6 y se accede a ella por medio de la interfaz de la tarjeta de interfaz de red a partir de un explorador web compatible de la estación de administración. Para ver una lista de los exploradores web admitidos, consulte "Exploradores web admitidos".

RACADM	Ofrece acceso remoto al iDRAC6 por medio de una interfaz de línea de comandos. RACADM usa la dirección IP del iDRAC6 para ejecutar comandos RACADM.
	
	NOTA: La opción de capacidad remota de racadm sólo se admite en las estaciones de administración. Para obtener más información, consulte "Uso de RACADM de manera remota".
	
	NOTA: Al utilizar la capacidad remota de racadm, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo:
	
	`racadm getconfig -f <nombre de archivo>`
	
	`o bien:`
	
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt subcomandos`

Consola Telnet	Proporciona acceso al iDRAC6 y compatibilidad con los comandos seriales y RACADM, incluidos los comandos **powerdown**, **powerup**, **powercycle** y **hardreset**. **NOTA:** Telnet es un protocolo no seguro que transmite todos los datos —incluso las contraseñas— en texto simple. Cuando transmita información confidencial, utilice la interfaz SSH.
Interfaz SSH	Proporciona las mismas capacidades que la consola Telnet a través de una capa de transporte cifrada que brinda mayor seguridad.
Interfaz IPMI	Brinda acceso a las funciones de administración básicas del sistema remoto por medio del iDRAC6. La interfaz incluye IPMI mediante LAN, IPMI mediante conexión serie y conexión serie mediante LAN. Para obtener más información, consulte la *Guía del usuario de utilidades del controlador de administración de la placa base de Dell OpenManage* en **support.dell.com\manuals**.

NOTA: El nombre de usuario predeterminado del iDRAC6 es `root` y la contraseña predeterminada es `calvin`.

Puede acceder a la interfaz web del iDRAC6 mediante la tarjeta de interfaz de red del iDRAC6 utilizando un explorador web admitido o mediante Server Administrator o IT Assistant.

Para acceder a la interfaz de acceso remoto del iDRAC6 por medio de Server Administrator, realice el siguiente procedimiento:

- Inicie Server Administrator.
- En el árbol de sistema que se encuentra en el panel a la izquierda de la página de inicio de Server Administrator, haga clic en **Sistema**→ **Chasis del sistema principal**→ **Controlador de acceso remoto**.

Para obtener más información, consulte la *Guía del usuario de Server Administrator*.

Uso de RACADM de manera remota

NOTA: Configure la dirección IP en el iDRAC6 antes de usar la capacidad remota de RACADM. Para obtener más información sobre cómo configurar el iDRAC6 y una lista de los documentos relacionados, consulte "Instalación básica de un iDRAC6".

RACADM proporciona una opción de capacidad remota (**-r**) que le permite conectarse al sistema administrado y ejecutar subcomandos RACADM desde una consola remota o una estación de administración. Para usar la capacidad remota, necesita un nombre de usuario válido (opción **-u**) y una contraseña (opción **-p**), así como la dirección IP del iDRAC6.

NOTA: Si el sistema desde el que está accediendo al sistema remoto no tiene un certificado de iDRAC6 en el almacén predeterminado de certificados, aparecerá un mensaje cuando escriba un comando de RACADM. Para obtener más información sobre los certificados de iDRAC6, consulte "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales".

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio

Ejecución continua. Utilice la opción -S para que racadm detenga la ejecución al producirse errores relacionados con certificados.)
```

RACADM continúa ejecutando el comando. No obstante, si utiliza la opción –S, RACADM detendrá la ejecución del comando y mostrará el siguiente mensaje:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

ERROR: Unable to connect to iDRAC6 at specified IP address

(Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio

Racadm detiene la ejecución del comando.

ERROR: no es posible establecer conexión con el iDRAC6 en la dirección IP especificada)
```

NOTA: La capacidad remota de RACADM sólo se admite en las estaciones de administración. Para obtener más información, consulte la *matriz de compatibilidad de software de los sistemas Dell* que se encuentra en la sección **OpenManage Software de Dell** en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

NOTA: Al utilizar la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo:

```
racadm getconfig -f <nombre de archivo>
```

O bien:

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt subcomandos
```

Sinopsis de RACADM

```
racadm -r <dirección IP del iDRAC6> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6> <subcomando> <opciones del subcomando>
```

Por ejemplo:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del iDRAC6 se ha cambiado a un puerto personalizado diferente al puerto predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP del iDRAC6>:<puerto> -u <nombre_de_usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6>:<puerto> <subcomando> <opciones del subcomando>
```

Opciones de RACADM

La Tabla 5-14 muestra una lista de las opciones del comando RACADM.

Tabla 5-14. Opciones del comando racadm

Opción	Descripción
-**r <*racIpAddr*>** -**r <*racIpAddr*>:<*número de puerto*>**	Especifica la dirección IP remota del controlador. Use <*número de puerto*> si el número de puerto del iDRAC6 no es el puerto predeterminado (443)
-**i**	Indica a RACADM que pregunte interactivamente al usuario el nombre de usuario y la contraseña.
-**u <*usrName*>**	Especifica el nombre de usuario que se usa para autenticar la transacción del comando. Si se usa la opción **-u**, se debe usar la opción **-p** y la opción **-i** (interactiva) no se permite.
-**p <*password*>**	Especifica la contraseña usada para autenticar la transacción del comando. Si se usa la opción **-p**, la opción **-i** no se permite.
-S	Indica que RACADM debe verificar si existen errores por certificados no válidos. RACADM detiene la ejecución del comando y

	muestra un mensaje de error si detecta un certificado no válido.

Activación y desactivación de la capacidad remota de RACADM

NOTA: Se recomienda ejecutar estos comandos en el sistema local.

La capacidad de RACADM remota está activada de manera predeterminada. Si se desactiva, escriba el siguiente comando de RACADM para activarla:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

Para desactivar la capacidad remota, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

Subcomandos de RACADM

La Tabla 5-15 proporciona la descripción de cada uno de los subcomandos de RACADM que puede ejecutar en RACADM. Para ver una lista detallada de los subcomandos de RACADM que incluye la sintaxis y las entradas válidas, consulte "Generalidades de los subcomandos de RACADM".

Al introducir un subcomando de RACADM, preceda el comando con racadm, por ejemplo.

```
racadm help
```

Tabla 5-15. Subcomandos de RACADM

Comando	Descripción
help	Lista los subcomandos del iDRAC6.
help *<subcomando>*	Muestra la descripción de uso del subcomando especificado.
arp	Muestra el contenido de la tabla ARP. Las entradas de la tabla ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la pantalla de último ASR (bloqueo) (la última pantalla azul).
clrraclog	Borra el registro del iDRAC6. Sólo se hace una entrada para indicar el usuario y la hora en la que se borró el registro.
config	Configura el iDRAC6.
getconfig	Muestra las propiedades de configuración actuales del iDRAC6.
coredump	Muestra el último volcado de núcleo del iDRAC6.
coredumpdelete	Borra el volcado del núcleo almacenado en el iDRAC6.
fwupdate	Ejecuta o muestra el estado de las actualizaciones del firmware del iDRAC6.
getssninfo	Muestra información sobre las sesiones activas.
getsysinfo	Muestra información general del iDRAC6 y del sistema.
getractime	Muestra la hora del iDRAC6.
ifconfig	Muestra la configuración actual de IP del iDRAC6.
netstat	Muestra la tabla de encaminamiento y las conexiones actuales.
ping	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de encaminamiento.
setniccfg	Establece la configuración IP para el controlador.
getniccfg	Muestra la configuración IP actual del controlador.
getsvctag	Muestra las etiquetas de servicio.
racdump	Vacía información del estado y la condición del iDRAC6 para la depuración de errores.
racreset	Restablece el iDRAC6.
racresetcfg	Restablece la configuración predeterminada del iDRAC6.
serveraction	Realiza operaciones de administración de energía en el sistema administrado.
getraclog	Muestra el registro del iDRAC6.
clrsel	Borra las entradas del registro de eventos del sistema.
gettracelog	Muestra el registro de rastreo del iDRAC6. Si se usa con -i, el comando muestra el número de entradas en el registro de rastreo del iDRAC6.
sslcsrgen	Genera y descarga la CSR de SSL.
sslcertupload	Carga un certificado de CA o un certificado de servidor en el iDRAC6.
sslcertdownload	Descarga un certificado de CA.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el iDRAC6.
sslkeyupload	Obliga al iDRAC6 a enviar un mensaje de correo electrónico de prueba a través de la tarjeta de interfaz de red del iDRAC6 para comprobar la configuración de correo electrónico.
testtrap	Obliga al iDRAC6 a enviar una excepción SNMP de prueba a través de la tarjeta de interfaz de red del iDRAC6 para comprobar la configuración de excepciones.

vmdisconnect	Obliga el cierre de la conexión de medios virtuales.
vmkey	Restablece el tamaño predeterminado de la memoria flash virtual (256 MB).

Preguntas frecuentes sobre los mensajes de error de RACADM

Tras realizar un restablecimiento del iDRAC6 (con el comando racadm racreset), escribo un comando y aparece el mensaje siguiente:

ERROR: Unable to connect to RAC at specified IP address (ERROR: no es posible establecer conexión con el RAC en la dirección IP especificada)

¿Qué significa este mensaje?

Debe esperar hasta que el iDRAC6 haya completado el restablecimiento antes de ejecutar otro comando.

Cuando uso los comandos y subcomandos de racadm, recibo mensajes de error que no entiendo.

Es posible que reciba uno o más de los siguientes errores cuando use los comandos y subcomandos de RACADM:

- Mensajes de errores de RACADM local: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de errores de RACADM remoto: problemas tales como una dirección IP, un nombre de usuario o una contraseña incorrectos.

Cuando ejecuto el comando ping con la dirección IP del iDRAC6 desde mi sistema y luego cambio mi iDRAC6 entre los modos Dedicado y Compartido durante la respuesta del comando ping, no recibo respuesta.

Borre la tabla ARP en el sistema.

Configuración de múltiples controladoras iDRAC6

Por medio de RACADM, usted puede configurar una o más controladoras iDRAC6 con propiedades idénticas. Cuando realiza una consulta en una controladora iDRAC6 especifica con las identificaciones de grupo y de objeto de la tarjeta, RACADM crea el archivo de configuración **racadm.cfg** a partir de la información obtenida. Si exporta el archivo a uno o varios iDRAC6, puede configurar las controladoras con propiedades idénticas en una cantidad de tiempo mínima.

NOTA: Algunos archivos de configuración contienen información exclusiva del iDRAC6 (como la dirección IP estática) que debe modificarse antes de exportar el archivo a otros iDRAC6.

Para configurar múltiples controladoras iDRAC6, realice los siguientes procedimientos:

1. Utilice RACADM para consultar el iDRAC6 de destino que contiene la configuración adecuada.

   NOTA: El archivo **.cfg** generado no contiene contraseñas de usuario.

   Abra una petición de comandos y escriba:

   ```
   racadm getconfig -f miarchivo.cfg
   ```

   NOTA: La redirección de la configuración del iDRAC6 hacia un archivo por medio de **getconfig -f** sólo se admite con las interfaces local y remota de RACADM.

2. Modifique el archivo de configuración con un editor de textos simple (opcional).

3. Utilice el nuevo archivo de configuración para modificar un iDRAC6 de destino.

   En la petición de comandos, escriba:

   ```
   racadm config -f miarchivo.cfg
   ```

4. Restablezca el iDRAC6 de destino que fue configurado.

   En la petición de comandos, escriba:

   ```
   racadm racreset
   ```

El subcomando **getconfig -f racadm.cfg** solicita la configuración del iDRAC6 y genera el archivo **racadm.cfg**. Si se requiere, puede configurar el archivo con otro nombre.

Puede usar el comando **getconfig** para ejecutar las siguientes acciones:

- Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice)
- Mostrar todas las propiedades de configuración de usuario por nombre de usuario

El subcomando **config** carga la información en otros iDRAC6. Utilice **config** para sincronizar la base de datos de usuarios y contraseñas con Server Administrator.

El usuario asigna el nombre al archivo de configuración inicial, **racadm.cfg**. En el siguiente ejemplo, el archivo de configuración se denomina **miarchivo.cfg**.

Para crear este archivo, escriba lo siguiente en la petición de comandos:

```
racadm getconfig -f miarchivo.cfg
```

PRECAUCIÓN: Se recomienda que edite este archivo con un editor de textos simple. La utilidad RACADM utiliza un analizador de textos ASCII. Los elementos de formato confunden al analizador y esto puede dañar la base de datos de RACADM.

Creación de un archivo de configuración del iDRAC6

El archivo de configuración del iDRAC6 **<***nombre_de_archivo***>.cfg** se utiliza con el comando `racadm config -f <nombre_de_archivo>.cfg`. Puede usar el archivo de configuración para crear un archivo de configuración (parecido a un archivo **.ini**) y configurar el iDRAC6 a partir de este archivo. Usted puede usar cualquier nombre de archivo y el archivo no requiere una extensión **.cfg** (aunque en este apartado nos refiramos al mismo con dicha extensión).

El archivo **.cfg** se puede:

- Crear
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg`
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y después modificarse

NOTA: Consulte "getconfig" para obtener información sobre el comando **getconfig**.

El archivo **.cfg** se analiza primero para verificar que los nombres de grupo y de objeto sean válidos y que se sigan algunas reglas simples de sintaxis. Los errores se señalan con el número de la línea en la que se detectó el error y un mensaje simple explica el problema. El archivo completo se analiza para confirmar que sea correcto y se muestran todos los errores. Los comandos de escritura no se transmiten al iDRAC6 si se encuentra un error en el archivo **.cfg**. El usuario debe corregir *todos* los errores antes de que pueda realizar cualquier configuración. La opción **-c** se puede usar en el subcomando **config**, que verifica sólo la sintaxis y no realiza operaciones de escritura en el iDRAC6.

Utilice las siguientes directrices al crear un archivo **.cfg**:

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

  El analizador lee en todos los índices del iDRAC6 para ese grupo. Los objetos dentro de dicho grupo son modificaciones simples cuando se configura el iDRAC6. Si un objeto modificado representa un índice nuevo, el índice se crea en el iDRAC6 durante la configuración.

- No se puede especificar el índice que se desea en un archivo **.cfg**.

  Los índices se pueden crear y eliminar, por lo que con el tiempo el grupo se puede fragmentar con índices usados y no usados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método permite tener flexibilidad al momento de agregar entradas indexadas en las que usted no necesita hacer coincidencias exactas de índice entre todos los RAC que se administran. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo **.cfg** que se analiza y se ejecuta correctamente en un iDRAC6 no funcione correctamente en otro si todos los índices están llenos y se tiene que agregar un nuevo usuario.

- Use el subcomando **racresetcfg** para configurar múltiples iDRAC6 con propiedades idénticas.

  Use el subcomando **racresetcfg** para restablecer el iDRAC6 a los valores predeterminados originales y luego ejecute el comando `racadm config -f <nombre_de_archivo>.cfg`. Asegúrese que el archivo **.cfg** tenga todos los objetos, usuarios, índices y demás parámetros requeridos.

PRECAUCIÓN: Use el subcomando racresetcfg para restablecer la base de datos y la configuración de la tarjeta de interfaz de red del iDRAC6 a los valores predeterminados originales y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas del análisis

- Todas las líneas que comienzan con '#' son tratadas como comentarios.

  Una línea de comentario *debe* comenzar en la columna uno. Un carácter "#" en cualquier otra columna se trata como un carácter "#".

  Algunos parámetros de módem pueden incluir caracteres # en la cadena. No se requiere un carácter de escape. Es posible que desee generar un archivo **.cfg** a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y luego realizar un comando `racadm config -f <nombre_de_archivo>.cfg` para un iDRAC6 diferente, sin agregar caracteres de escape.

  Ejemplo:

  ```
  #

  # This is a comment (Esto es un comentario)

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<# de inicio de módem, no es un comentario>
  ```

- Todas las entradas de grupo deben estar rodeadas por los caracteres "**[**"y "**]**".

  El carácter "**[**" de inicio que denota un nombre de grupo *debe* comenzar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

Ejemplo:

```
[cfgLanNetworking] -{nombre de grupo}

cfgNicIpAddress=143.154.133.121 {nombre de objeto}
```

- Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor.

  Se ignorarán los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de una cadena de valores se mantienen sin modificación. Los caracteres a la derecha del símbolo "=" se tomarán tal cual (por ejemplo, un segundo "=" o un símbolo "#", "[", "]", etc.). Todos estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

  Consulte el ejemplo en el punto anterior.

- El analizador del archivo **.cfg** ignora una entrada de objeto de índice.

  El usuario *no puede* especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva entrada en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <nombre del archivo>.cfg` coloca un comentario delante de los objetos de índice, lo que permite al usuario ver los comentarios incluidos.

NOTA: Usted puede crear un grupo indexado manualmente, con el siguiente comando:
`racadm config -g <nombre_de_grupo> -o <objeto anclado> -i <indice 1-16> <nombre de ancla exclusivo>`

- La línea de un grupo indexado *no se puede* eliminar de un archivo **.cfg**.

  El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

  ```
  racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> -i <indice de 1 a 16> ""
  ```

NOTA: Una cadena NULA (que se identifica por dos caracteres "") indica al iDRAC6 que elimine el índice del grupo especificado.

Para ver el contenido de un grupo indexado, use el siguiente comando:

```
racadm getconfig -g <nombre_de_grupo> -i <indice de 1 a 16>
```

- Para grupos indexados, el ancla de objeto *debe ser* el primer objeto después del par de corchetes ([ ]). Los siguientes son ejemplos de los grupos indexados actuales:

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
  ```

  Si escribe `racadm getconfig -f <mi_ejemplo>.cfg`, el comando genera un archivo **.cfg** para la configuración actual del iDRAC6. Este archivo de configuración se puede usar como ejemplo y como punto de partida para su archivo **.cfg** exclusivo.

Modificación de la dirección IP del iDRAC6

Al modificar la dirección IP del iDRAC6 en el archivo de configuración, elimine todas las entradas innecesarias de **<***variable***>**=**valor**. Sólo permanece la etiqueta del grupo variable real con "[" y "]", incluidas las dos entradas **<***variable***>**=**valor** que pertenecen al cambio de dirección IP.

Por ejemplo:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (comentario, el resto de esta línea se ignora)

cfgNicGateway=10.35.9.1
```

El comando **racadm config -f mi_archivo.cfg** analiza el archivo e identifica todos los errores por número de línea. Un archivo correcto actualizará las entradas adecuadas. Además, usted puede usar el mismo comando **getconfig** que se usó en el ejemplo anterior para confirmar la actualización.

Utilice este archivo para descargar cambios que abarcan toda la empresa o para configurar nuevos sistemas en la red.

NOTA: "Anchor" es un término interno y no se debe utilizar en el archivo.

Configuración de las propiedades de red del iDRAC6

Para generar una lista de las propiedades disponibles de red, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Para utilizar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** y active esta función:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

Los comandos brindan la misma funcionalidad de configuración que la utilidad de configuración del iDRAC6 al momento de inicio cuando se pide que presione <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, consulte Configuración de su sistema para usar el iDRAC6.

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de red LAN deseadas.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN del iDRAC6 se desactivará aun cuando DHCP esté activado.

Modos de iDRAC6

El iDRAC6 puede configurarse en uno de cuatro modos:

- Dedicado
- Compartido
- Compartido con LOM2 de protección contra fallas
- Compartido con todos los LOM2 de protección contra fallas

La Tabla 5-16 ofrece una descripción de cada modo.

Tabla 5-16. Configuraciones de la tarjeta de interfaz de red del iDRAC6

Modo	Descripción
Dedicado	El iDRAC6 utiliza su propia tarjeta de interfaz de red (conector RJ-45) y la dirección MAC del iDRAC para el tráfico de red.
Compartido	El iDRAC6 usa LOM1 en la placa madre.
Compartido con LOM2 de protección contra fallas	El iDRAC6 utiliza LOM1 y LOM2 como equipo para protección contra fallas. El equipo utiliza la dirección MAC del iDRAC6.
Compartido con todos los LOM2 de protección contra fallas	El iDRAC6 usa LOM1, LOM2, LOM3 y LOM4 como equipo para protección contra fallas. El equipo utiliza la dirección MAC del iDRAC6.

Preguntas frecuentes sobre seguridad de red

Al acceder a la interfaz web del iDRAC6, recibo una advertencia de seguridad que advierte que el nombre de host del certificado SSL no coincide con el nombre de host del iDRAC6.

El iDRAC6 incluye un certificado de servidor del iDRAC6 predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Cuando se usa este certificado, el explorador web muestra una advertencia de seguridad porque el certificado predeterminado se emite para el **certificado predeterminado del iDRAC6**, que no coincide con el nombre del host del iDRAC6 (por ejemplo, la dirección IP).

Para solucionar este problema de seguridad, cargue un certificado de servidor del iDRAC6 emitido para la dirección IP o el nombre de iDRAC del iDRAC6. Cuando se genere la solicitud de firma del certificado (CSR) que se usará para emitir el certificado, asegúrese de que el nombre común (CN) del CSR concuerde con la dirección IP (**si el certificado se emite para la IP**) del iDRAC6 (por ejemplo, 192.168.0.120) o el nombre DNS registrado del iDRAC6 (**si el certificado se emite al nombre registrado de iDRAC**).

Para asegurarse de que la CSR coincida con el nombre DNS registrado del iDRAC6:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y haga clic en **Red**.
3. En la tabla **Valores comunes**:
   a. Seleccione la casilla de verificación **Registrar el iDRAC en DNS**.
   b. En el campo **Nombre del iDRAC en DNS**, introduzca el nombre del iDRAC6.
4. Haga clic en **Aplicar cambios**.

Consulte "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales" para obtener más información sobre cómo generar CSR y cómo emitir certificados.

¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?

Es posible que los servicios de RACADM remoto y la interfaz web tarden un poco en estar disponibles después de restablecer el servidor web del iDRAC6.

El servidor web del iDRAC6 se restablece después de los siguientes acontecimientos:

- Cuando la configuración de red o las propiedades de seguridad de la red se cambian mediante la interfaz web de usuario del iDRAC6
- Cuando la propiedad **cfgRacTuneHttpsPort** cambia (incluso cuando un comando config -f <*archivo_de_config*> la cambia)
- Cuando se utiliza **racresetcfg**
- Cuando el iDRAC6 se restablece
- Cuando se carga un nuevo certificado de servidor SSL

¿Por qué mi servidor DNS no registra mi iDRAC6?

Algunos de los servidores DNS sólo registran nombres de 31 caracteres o menos.

Al acceder a la interfaz web del iDRAC6, recibo una advertencia de seguridad que informa que el certificado SSL fue emitido por una autoridad de certificados (CA) que no es confiable.

El iDRAC6 incluye un certificado de servidor del iDRAC6 predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Este certificado no fue emitido por una CA confiable. Para resolver este asunto de seguridad, cargue un certificado de servidor del iDRAC6 que haya sido publicado por una CA confiable (por ejemplo, Microsoft Certificate Authority, Thawte o Verisign). Consulte "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales" para obtener más información acerca de la emisión de certificados.

Regresar a la página de contenido

Regresar a la página de contenido

Cómo agregar y configurar usuarios del iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Para administrar el sistema con el iDRAC6 y mantener la seguridad del sistema, cree usuarios exclusivos con permisos administrativos específicos (o *con autoridad basada en funciones*). Para obtener seguridad adicional, también puede configurar alertas que se envían por correo electrónico a usuarios específicos cuando ocurre un evento determinado en el sistema.

Uso de la interfaz web para configurar usuarios del iDRAC6

Cómo agregar y configurar usuarios del iDRAC6

Para administrar el sistema con el iDRAC6 y mantener la seguridad del sistema, cree usuarios exclusivos con permisos administrativos específicos (o *con autoridad basada en funciones*).

Para agregar y configurar usuarios del iDRAC6, realice los pasos a continuación:

NOTA: Debe tener permiso para **Configurar usuarios** para cambiar un usuario del iDRAC.

1. Haga clic en **Acceso remoto**→ **Configuración**→ **Usuarios**.

   La página Usuarios muestra la siguiente información para los usuarios del iDRAC: **ID de usuario, Estado (Activado/Desactivado), Nombre del usuario, Privilegios RAC**, **Privilegios LAN de IPMI**, **Privilegio serial de IPMI** y estado de **Serial sobre LAN (Activado/Desactivado)**. La Tabla 6-1 describe los estados y permisos del usuario para configurar usuarios del iDRAC.

   NOTA: El usuario 1 está reservado para el usuario anónimo de IPMI y no se puede configurar.

2. En la columna **Id. de usuario**, haga clic en un número de identificación de usuario.

   En la página del **Menú principal del usuario**, puede configurar un usuario, ver un certificado de usuario, cargar un certificado de confianza de una autoridad de certificados (CA) o ver un certificado de confianza de una CA.

   Si selecciona la opción **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página Configuración de usuario. Pase al paso 4.

   Si selecciona una opción en **Configuración de tarjeta inteligente**, consulte la Tabla 6-2.

3. En la página **Configuración de usuario**, configure lo siguiente:
   - El nombre de usuario, la contraseña y los permisos de acceso para un usuario nuevo o existente del iDRAC. La Tabla 6-3 describe **Configuración global de usuario**.
   - Los privilegios IPMI del usuario. La Tabla 6-4 describe los **Privilegios de usuario de IPMI** necesarios para configurar los privilegios de LAN del usuario.
   - Los privilegios de usuario del iDRAC. La Tabla 6-5 describe los **Privilegios de usuario del iDRAC**.
   - Permisos de acceso de grupo del iDRAC. La Tabla 6-6 describe los **Permisos de grupo del iDRAC.**

4. Cuando termina, haga clic en **Aplicar cambios**.

5. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 6-7.

Tabla 6-1. Estados y permisos de usuario

Valor	Descripción
Identificación de usuario	Muestra la lista secuencial de los números de identificación de usuarios. Cada campo en **Identificación de usuario** contiene uno de los 16 números de identificación de usuario predefinidos. Este campo no se puede editar.
Estado	Muestra el estado de inicio de sesión del usuario: Activado o Desactivado. (Desactivado es el valor predeterminado). **NOTA:** El usuario 2 está activado de manera predeterminada.
Nombre de usuario	Muestra el nombre de inicio de sesión del usuario. Especifica un nombre de usuario del iDRAC6 de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único.

	NOTA: Los nombres de usuario del iDRAC6 no pueden incluir los caracteres **/** (diagonal) ni **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Privilegio RAC	Muestra el grupo (nivel de privilegio) al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
Privilegio LAN de IPMI	Muestra el nivel de privilegio LAN de IPMI al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
Privilegio serial de IPMI	Muestra el nivel de privilegio del puerto serial de IPMI al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
Comunicación en serie en la LAN	Permite o revoca el permiso al usuario de usar la comunicación en serie en la LAN de IPMI.

Tabla 6-2. Opciones de configuración de la tarjeta inteligente

Opción	Descripción
Ver certificado de usuario	Muestra la página de certificado de usuario que se cargó en el iDRAC.
Cargar certificado de CA de confianza	Permite cargar el certificado de CA de confianza en el iDRAC e importarlo al perfil del usuario.
Ver certificado de CA de confianza	Muestra el certificado de CA de confianza que se cargó en el iDRAC. El certificado de CA de confianza lo emite la CA que está autorizada para emitir certificados para usuarios.

Tabla 6-3. Configuración general de usuarios

Identificación de usuario	Uno de los 16 números preconfigurados de identificación de usuario.
Activar el usuario	Cuando está seleccionado, indica que el acceso del usuario al iDRAC6 está activado. Cuando no está seleccionado, el acceso de usuario está desactivado.
Nombre de usuario	Un nombre de usuario de hasta 16 caracteres.
Cambiar contraseña	Activa los campos **Nueva contraseña** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán.
Confirmar nueva contraseña	Vuelva a escribir la contraseña del usuario del iDRAC para confirmarla.

Tabla 6-4. Privilegios del usuario de IPMI

Propiedad	Descripción
Privilegio máximo permitido de usuario de LAN	Especifica el privilegio máximo en el canal de LAN de IPMI para uno de los siguientes grupos de usuarios: **Administrador**, **Operador**, **Usuario o Ninguno**.
Privilegio máximo permitido de usuario de puerto serie	Especifica el privilegio máximo en el canal de conexión serie de IPMI para uno de los siguientes grupos de usuarios: **Administrador**, **Operador**, **Usuario o Ninguno**.
Activar comunicación en serie en la LAN.	Permite al usuario usar la comunicación en serie en la LAN de IPMI. Cuando está seleccionado, este privilegio está activado.

Tabla 6-5. Privilegios del usuario del iDRAC

Propiedad	Descripción
Funciones	Especifica el privilegio máximo de usuario del iDRAC del usuario a uno de los siguientes: **Administrador**, **Operador**, **Sólo lectura** o **Ninguno**. Consulte la Tabla 6-6 para ver los **Permisos del grupo del iDRAC**.
Iniciar sesión en el iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar el iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Permite al usuario otorgar permisos de acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros del iDRAC.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de control del servidor.
Acceder a redirección de consola	Permite al usuario ejecutar la redirección de consola.
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Tabla 6-6. Permisos de grupo del iDRAC

Grupo de usuarios	Permisos concedidos
Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.
Operador	Selecciona cualquier combinación de los permisos siguientes: **Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de acción del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**
Sólo lectura	**Iniciar sesión en el iDRAC**
Ninguno	Sin permisos asignados

Tabla 6-7. Botones de la página de configuración de usuario

Botón	Acción
Imprimir	Imprime los valores de la **Configuración de usuario** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de usuario**.
Volver a la página de usuarios	Regresa a la **página de usuarios**.
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la configuración de usuario.

Uso de la utilidad RACADM para configurar usuarios del iDRAC6

NOTA: Se debe haber iniciado sesión como usuario **root** para ejecutar los comandos de RACADM en un sistema remoto con Linux.

Es posible configurar uno o varios usuarios del iDRAC6 por medio de la línea de comandos RACADM que se instala con los agentes del iDRAC6 en el sistema administrado.

Para configurar varios iDRAC6 con valores de configuración idénticos, realice uno de los siguientes procedimientos:

- Use los ejemplos de RACADM en esta sección como guía para crear un archivo de procesamiento en lote de comandos RACADM y después ejecute el archivo de procesamiento en lote en cada sistema administrado.
- Cree un archivo de configuración del iDRAC6 según se describe en "Generalidades de los subcomandos de RACADM" y ejecute el subcomando **racadm config** en cada sistema administrado por medio del mismo archivo de configuración.

Antes de comenzar

Puede configurar hasta 16 usuarios en la base de datos de propiedades del iDRAC6. Antes de activar manualmente a un usuario del iDRAC6, verifique si existe algún usuario actual. Si está configurando un iDRAC6 nuevo o si ha ejecutado el comando **racadm racresetcfg**, el único usuario actual es root con la contraseña calvin. El subcomando **racresetcfg** restablece los valores predeterminados originales del iDRAC6.

PRECAUCIÓN: Tenga cuidado cuando utilice el comando racresetcfg, pues con éste se restablecen los valores predeterminados de *todos* los parámetros de configuración. Todos los cambios anteriores se perderán.

NOTA: Los usuarios se pueden activar o desactivar posteriormente. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC6.

Para verificar si existe un usuario, escriba el comando siguiente en la petición de comandos:

```
racadm getconfig -u <nombre_de_usuario>
```

O bien:

escriba el comando siguiente una vez para cada índice de 1 a 16:

```
racadm getconfig -g cfgUserAdmin -i <índice>
```

NOTA: También puede escribir racadm getconfig -f <mi_archivo.cfg> y ver o editar el archivo **mi_archivo.cfg**, que incluye todos los parámetros de configuración del iDRAC6.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

Si el objeto **cfgUserAdminUserName** no tiene un valor, el número de índice que indica el objeto **cfgUserAdminIndex** está disponible para su uso. Si aparece un nombre después del signo "=", ese nombre de usuario tomará ese índice.

NOTA: Cuando activa o desactiva un usuario manualmente con el subcomando **racadm config**, *debe especificar* el índice con la opción -**i**. Note que el objeto **cfgUserAdminIndex** mostrado en el ejemplo anterior contiene un carácter '#'. Asimismo, si utiliza el comando **racadm config** -**f racadm.cfg** para especificar el número de grupos/objetos por escribir, el índice no se podrá especificar. Se agrega un nuevo usuario al primer índice disponible. Este

comportamiento permite tener más flexibilidad al configurar múltiples iDRAC6 con los mismos valores.

Cómo agregar un usuario del iDRAC6

Para agregar un nuevo usuario a la configuración del RAC, se pueden usar unos cuantos comandos básicos. En general, realice los siguientes procedimientos:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los siguientes privilegios del usuario:
   - Privilegio iDRAC
   - Privilegio LAN de IPMI
   - Privilegio Serial de IPMI
   - Privilegio de comunicación serial en LAN
4. Active el usuario.

Ejemplo

El siguiente ejemplo describe cómo agregar un nuevo usuario de nombre "Juan" con la contraseña "123456" y privilegios de inicio de sesión en el RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Para verificarlo, use uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig –g cfgUserAdmin –i 2
```

Eliminación de un usuario del iDRAC6

Al usar RACADM, los usuarios se deben desactivar manual e individualmente. Los usuarios no se pueden eliminar por medio de un archivo de configuración.

El ejemplo siguiente ilustra la sintaxis de comando que se puede usar para eliminar un usuario de RAC:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <índice> ""
```

Una cadena nula de dos caracteres de comillas ("") indica al iDRAC6 que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.

Activación de un usuario del iDRAC6 con permisos

Para activar un usuario con permisos administrativos específicos (autoridad en base a funciones), encuentre primero un índice de usuario disponible por medio de los pasos de la sección "Antes de comenzar". Posteriormente, escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña.

NOTA: Consulte la Tabla B-2 para ver una lista de los valores válidos de máscara de bits para los privilegios de usuario específicos. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios habilitados.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <índice> <valor de máscara de bits de privilegios de usuario>
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso del iDRAC6 con Microsoft Active Directory

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Un servicio de directorio se usa para mantener una base de datos común de toda la información necesaria para controlar usuarios, equipos, impresoras, etc. en una red. Si la empresa ya utiliza el software de servicio Microsoft® Active Directory®, puede configurarlo para que proporcione acceso al iDRAC6, lo que le permite agregar privilegios de usuario del iDRAC6 a los usuarios existentes y controlar estos privilegios en el software Active Directory.

NOTA: El uso de Active Directory para reconocer usuarios del iDRAC6 se admite en los sistemas operativos Microsoft Windows® 2000, Windows Server® 2003 y Windows Server 2008.

La Tabla 7-1 muestra los nueve privilegios de usuario de Active Directory del iDRAC6.

Tabla 7-1. Privilegios de usuario del iDRAC6

Privilegio	Descripción
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC6.
Configurar iDRAC	Permite al usuario configurar el iDRAC6.
Configurar usuarios	Permite al usuario otorgar acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros del iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a redirección de consola	Permite al usuario ejecutar la redirección de consola.
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Requisitos previos para activar la autenticación de Active Directory para el iDRAC6

Para usar la función de autenticación de Active Directory del iDRAC6, debe haber implementado una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener información sobre cómo configurar una infraestructura de Active Directory si aún no tiene una.

El iDRAC6 utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para autenticar de manera segura en Active Directory; por lo tanto, necesitará también una PKI integrada en la infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener más información sobre la configuración de PKI.

Para autenticar correctamente todos los controladores de dominio, también es necesario activar la capa de sockets seguros (SSL) en todos los controladores de dominio con los que el iDRAC6 se conecta. Consulte "Activación de SSL en un controlador de dominio" para obtener información más específica.

Mecanismos de autenticación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: mediante la solución de *esquema ampliado*, que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell. También puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las secciones siguientes para obtener más información sobre estas soluciones.

Cuando se usa Active Directory para configurar el acceso al iDRAC6, se debe elegir la solución de esquema ampliado o de esquema estándar.

Las ventajas de usar la solución de esquema ampliado son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Se permite la configuración del acceso de los usuarios en diferentes iDRAC6 con diversos niveles de privilegio.

La ventaja de utilizar la solución de esquema estándar radica en que no se requiere una ampliación del esquema, ya que la configuración predeterminada del esquema de Active Directory que brinda Microsoft proporciona todas las clases de objetos necesarias.

Generalidades del esquema ampliado de Active Directory

Para utilizar la solución de esquema ampliado, es necesaria una ampliación de esquema de Active Directory según se describe en la siguiente sección.

Extensión del esquema de Active Directory

Importante: la ampliación del esquema para este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Deberá ampliar el nuevo esquema e instalar el nuevo complemento Microsoft Management Console (MMC) de usuarios y equipos de Active Directory en su directorio. El esquema anterior no funciona con este producto.

NOTA: La ampliación del nuevo esquema y la instalación de la nueva ampliación en el complemento de usuarios y equipos de Active Directory no afectan los productos anteriores.

Puede encontrar el complemento MMC de usuarios y equipos de Active Directory y la ampliación de esquema en el DVD *Dell Systems Management Tools and Documentation*. Para obtener más información, consulte "Extensión del esquema de Active Directory" e "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory". Para obtener más detalles sobre la ampliación del esquema para iDRAC6 y la instalación del complemento MMC de usuarios y equipos de Active Directory, consulte la *Guía del usuario de instalación y seguridad de Dell OpenManage* en **support.dell.com\manuals**.

NOTA: Cuando crea objetos de asociación o de dispositivo del iDRAC, asegúrese de seleccionar **Dell Remote Management Object Advanced**.

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden ampliar la base de datos de Active Directory al agregar sus propios atributos y clases únicos para solucionar necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autenticación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de Identificadores de Objeto de Active Directory (OID) de modo que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para ampliar el esquema en Microsoft Active Directory, Dell recibió OID exclusivos, extensiones de nombre exclusivas e identificaciones de atributo vinculadas exclusivamente para las clases y los atributos agregados al servicio de directorio.

La extensión de Dell es: dell

El OID base de Dell es: 1.2.840.113556.1.8000.1280

El rango del LinkID de RAC es: 12070 a 12079

Descripción de las extensiones de esquema del iDRAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha ampliado el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o los grupos que tienen un conjunto específico de privilegios para uno o varios dispositivos del iDRAC. Este modelo proporciona máxima flexibilidad al Administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC y dispositivos del iDRAC en la red sin aumentar demasiado la complejidad.

Descripción general de los objetos de Active Directory

Para cada uno de los iDRAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de iDRAC. Puede crear varios objetos de asociación, y cada objeto de asociación puede vincularse a cuantos usuarios, grupos de usuarios u objetos de dispositivo del iDRAC sean necesarios. Los usuarios y los grupos de usuarios del iDRAC pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación puede vincularse (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo del iDRAC) sólo a un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los iDRAC específicos.

El objeto de dispositivo del iDRAC es el vínculo al firmware del iDRAC para consultar Active Directory para autenticación y autorización. Cuando se agrega un iDRAC a la red, el administrador debe configurar el iDRAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autenticación y la autorización con Active Directory. Además, el administrador también debe agregar el iDRAC a por lo menos un objeto de asociación para que los usuarios se puedan autenticar.

La Figura 7-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

Figura 7-1. Configuración típica de los objetos de Active Directory

Usted puede crear tantos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo del iDRAC por cada iDRAC de la red que desea integrar con Active Directory para autenticación y autorización con iDRAC.

El objeto de asociación permite toda cantidad de usuarios o grupos, así como de objetos de dispositivo del iDRAC. Sin embargo, el objeto de asociación sólo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los *usuarios* con *privilegios* en los iDRAC.

La extensión de Dell al complemento MMC de usuarios y equipos de Active Directory sólo permite asociar el objeto de privilegio y los objetos del iDRAC del mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC de otro dominio se agregue como miembro del producto del objeto de asociación.

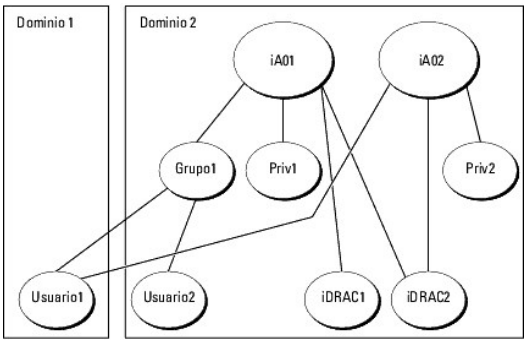
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema ampliado admiten todo tipo de grupos de usuarios o todo grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema ampliado

El mecanismo de autenticación del esquema ampliado admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados con el mismo usuario entre distintos objetos de asociación. En otras palabras, la autenticación del esquema ampliado acumula privilegios para permitir al usuario el súper conjunto de todos los privilegios asignados que corresponden a los distintos objetos de privilegio asociados al mismo usuario.

La Figura 7-2 muestra un ejemplo de la acumulación de privilegios por medio del esquema ampliado.

Figura 7-2. Acumulación de privilegios para un usuario



La figura muestra dos objetos de asociación: iA01 e iA02. El Usuario1 está asociado con el iDRAC2 por medio de ambos objetos de asociación. Por lo tanto, el Usuario1 ha acumulado privilegios que resultan de la combinación del conjunto de privilegios de los objetos Priv1 y Priv2 en el iDRAC2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; y Priv2 tiene los privilegios: Inicio de sesión en iDRAC, Configurar el iDRAC y Probar alertas. Como resultado, el Usuario1 tiene ahora el conjunto de privilegios: Inicio de sesión en iDRAC, Medios virtuales, Borrar registros, Configurar el iDRAC y Probar alertas, que es el conjunto de privilegios combinados de Priv1 y Priv2.

La autenticación del esquema ampliado acumula privilegios para permitir que el usuario tenga el conjunto máximo de privilegios según los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

En esta configuración, el Usuario1 tiene privilegios de Priv1 y Priv2 en iDRAC2. El Usuario1 tiene privilegios de Priv1 en iDRAC1 solamente. El Usuario2 tiene privilegios de Priv1 tanto en iDRAC1 como en iDRAC2. Además, esta ilustración muestra que el Usuario1 puede estar en un dominio diferente y ser miembro de un grupo anidado.

Configuración de Active Directory de esquema ampliado para acceder al iDRAC

Antes de usar Active Directory para acceder al iDRAC6, debe configurar el software Active Directory y el iDRAC6 llevando a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (consulte "Extensión del esquema de Active Directory").
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory").
3. Agregue usuarios del iDRAC6 y sus privilegios a Active Directory (consulte "Cómo agregar usuarios y privilegios del iDRAC a Active Directory").

4. Active SSL en cada uno de los controladores de dominio (consulte "Activación de SSL en un controlador de dominio").

5. Configure las propiedades de Active Directory del iDRAC6 por medio de la interfaz web del iDRAC6 o RACADM (consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema ampliado por medio de RACADM").

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

Puede ampliar el esquema por medio de uno de los métodos siguientes:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos LDIF

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation*, en los siguientes directorios respectivamente:

- *Unidad de DVD*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <Unidad **DVD >:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, consulte "Uso de Dell Schema Extender".

Puede copiar y ejecutar Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

NOTA: Dell Schema Extender utiliza el archivo **SchemaExtenderOem.ini**. Para asegurar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
2. Lea y comprenda la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Finalizar**.

   El esquema ha sido extendido. Para verificar la ampliación del esquema, utilice el complemento de esquema de Active Directory y MMC para controlar que existan los siguientes elementos:

   - Clases (consulte de la Tabla 7-2 a la Tabla 7-7)
   - Atributos (Tabla 7-8)

Consulte la documentación de Microsoft para obtener información acerca de cómo utilizar el complemento de esquema de Active Directory y MMC.

Tabla 7-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 7-3. Clase dellRacDevice

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
Descripción	Representa el dispositivo iDRAC de Dell. El dispositivo iDRAC debe estar configurado como delliDRACDevice en Active Directory. Esta configuración hace posible que el iDRAC envíe consultas de protocolo de acceso ligero de directorio (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	**dellSchemaVersion**

	dellRacType

Tabla 7-4. Clase delliDRACAssociationObject

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	**dellProductMembers** **dellPrivilegeMember**

Tabla 7-5. Clase dellRAC4Privileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Descripción	Se usa para definir los privilegios (derechos de autorización) del dispositivo iDRAC.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabla 7-6. Clase dellPrivileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	**dellRAC4Privileges**

Tabla 7-7. Clase dellProduct

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	**dellAssociationMembers**

Tabla 7-8. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/Descripción	**OID asignado/Identificador de objeto de sintaxis**	**Con un solo valor**
dellPrivilegeMember Lista de los objetos dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distinguido (LDAPTYPE_DN	FALSE

atributo es el vínculo de avance al vínculo de retroceso dellAssociationMembers. Identificación de vínculo: 12070	1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de redirección de consola en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignoran las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena en que se ignoran las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el enlace de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory

Cuando se amplía el esquema en Active Directory, también debe ampliarse el complemento de usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC, los usuarios y los grupos de usuarios, y las asociaciones y privilegios del iDRAC.

Cuando instala el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation*, puede ampliar el complemento si selecciona la opción **Complemento de usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener más instrucciones sobre la instalación del software de administración de sistemas. Para sistemas operativos Windows de 64 bits, el instalador del complemento se ubica en **<unidad DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**.

Para obtener más información acerca del complemento de usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Instalación del paquete de administrador

Debe instalar el paquete de administrador en cada sistema que administre los objetos del iDRAC de Active Directory. Si no instala el paquete de administrador, no podrá ver el objeto iDRAC de Dell en el contenedor.

Para obtener más información, consulte "Cómo abrir el complemento de usuarios y equipos de Active Directory".

Cómo abrir el complemento de usuarios y equipos de Active Directory

Para abrir el complemento de usuarios y equipos de Active Directory:

1. Si está conectado en el controlador del dominio, haga clic en **Inicio**Æ **Herramientas administrativas**→ **Usuarios y equipos de Active Directory**.

   Si no está conectado en el controlador de dominio, debe tener el paquete de administrador de Microsoft correspondiente instalado en el sistema local. Para instalar este paquete de administrador, haga clic en **Inicio**→ **Ejecutar**, escriba `MMC` y oprima **Entrar**.

   Aparecerá la consola MMC.

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).

3. Haga clic en **Agregar o quitar complemento**.

4. Seleccione el **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar**.

5. Haga clic en **Cerrar** y haga clic en **Aceptar**.

Cómo agregar usuarios y privilegios del iDRAC a Active Directory

El complemento de usuarios y equipos de Active Directory ampliado por Dell permite agregar usuarios y privilegios del iDRAC mediante la creación de objetos de asociación, privilegio e iDRAC. Para agregar cada tipo de objeto, realice los pasos a continuación:

- Cree un objeto de dispositivo del iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Configuración de un objeto de asociación

Creación de un objeto de dispositivo del iDRAC

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del ratón en un contenedor.

2. Seleccione **Nuevo**→ **Dell Remote Management Object Advanced**.

   Se abrirá la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC que usted va a escribir en el Paso A de "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6".

4. Seleccione **Objeto de dispositivo de iDRAC**.

5. Haga clic en **Aceptar**.

Creación de un objeto de privilegio

NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del ratón en un contenedor.

2. Seleccione **Nuevo**→ **Dell Remote Management Object Advanced**.

   Se abrirá la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto.

4. Seleccione **Objeto de privilegio**.

5. Haga clic en **Aceptar**.

6. Haga clic con el botón derecho del ratón en el objeto de privilegio que creó y seleccione **Propiedades**.

7. Haga clic en la lengüeta **Privilegios de administración remota** y seleccione los privilegios que desea otorgar al usuario.

Creación de un objeto de asociación

NOTA: El objeto de asociación del iDRAC se deriva de un grupo y su alcance está establecido en Local de dominio.

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del ratón en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Esto abrirá la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de asociación**.
5. Seleccione el ámbito para el **objeto de asociación**.
6. Haga clic en **Aceptar**.

Configuración de un objeto de asociación

En la ventana **Propiedades de objeto de asociación**, puede asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos del iDRAC.

Puede agregar grupos de usuarios. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

1. Haga clic con el botón derecho del ratón en el **objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la lengüeta **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de grupo de usuarios o usuario y haga clic en **Aceptar**.

Haga clic en la lengüeta **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentican en un dispositivo iDRAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

1. Seleccione la lengüeta **Objetos de privilegio** y haga clic en **Agregar**.
2. Escriba el nombre del objeto de privilegio y haga clic en **Aceptar**.

Haga clic en la lengüeta **Productos** para agregar un dispositivo iDRAC conectado a la red disponible para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de iDRAC a un objeto de asociación.

Cómo agregar dispositivos de iDRAC

Para agregar dispositivos de iDRAC:

1. Seleccione la lengüeta **Productos** y haga clic en **Agregar**.
2. Escriba el nombre del dispositivo iDRAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.

3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.

4. Haga clic en la lengüeta **Configuración** y seleccione **Active Directory**.

5. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparecerá la página **Paso 1 de 4** de **Configuración y administración de Active Directory**.

6. En **Configuración de certificados**, marque **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9.

7. En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado.

   NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

8. Haga clic en **Cargar**.

   Aparecerá la información del certificado de CA de Active Directory que se cargó.

9. En **Cargar Kerberos Keytab**, escriba la ruta de acceso del archivo keytab o bien explore el sistema para localizarlo. Haga clic en **Cargar**. El archivo keytab de Kerberos se cargará en el iDRAC6.

10. Haga clic en **Siguiente** para ir al **Paso 2 de 4** de **Configuración y administración de Active Directory**.

11. Haga clic en **Activar Active Directory**.

PRECAUCIÓN: En esta versión, las funciones de autenticación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el esquema ampliado.

12. Haga clic en **Agregar** para introducir el nombre de dominio de usuario.

13. Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**. Tenga en cuenta que este paso es opcional. Si configura una lista de dominios de usuario, la lista estará disponible en la pantalla de inicio de sesión de la interfaz web. Usted puede elegir de la lista y luego sólo debe escribir el nombre de usuario.

14. Escriba el **Tiempo de expiración** en segundos para especificar el tiempo que el iDRAC6 tendrá que esperar para las respuestas de Active Directory. El valor predeterminado es 120 segundos.

15. Escriba la dirección de servidor del controlador de dominio. Puede introducir hasta tres servidores Active Directory para procesar los inicios de sesión, pero es necesario que configure al menos un servidor. Para hacerlo, introduzca la dirección IP o el nombre de dominio completo (FQDN). iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.

16. Haga clic en **Siguiente** para ir al **Paso 3 de 4** de **Configuración y administración de Active Directory**.

17. En **Selección del esquema**, haga clic en **Esquema ampliado.**

18. Haga clic en **Siguiente** para ir al **Paso 4 de 4** de **Configuración y administración de Active Directory**.

19. En **Configuración del esquema ampliado**, escriba el nombre del iDRAC y el nombre de dominio para configurar el objeto de dispositivo del iDRAC. El nombre de dominio del iDRAC es el dominio en el que se crea el objeto del iDRAC.

20. Haga clic en **Finalizar** para guardar la configuración del esquema ampliado de Active Directory.

    El servidor web del iDRAC6 lo regresa automáticamente a la página **Configuración y administración de Active Directory**.

21. Haga clic en **Comprobar configuración** para controlar la configuración del esquema ampliado de Active Directory.

22. Escriba su nombre de usuario y contraseña de Active Directory.

    Visualizará los resultados de la prueba y el registro de la misma. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

    NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Haga clic en **Acceso remoto→ Configuración→ Red** para configurar los servidores DNS de forma manual o bien utilice DHCP para obtener los servidores DNS.

Con este paso se completa la configuración de Active Directory con esquema ampliado.

Configuración de Active Directory con esquema ampliado por medio de RACADM

Use los comandos siguientes para configurar el componente Active Directory del iDRAC con el esquema ampliado mediante la interfaz de línea de comandos de RACADM, en lugar de la interfaz web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 1
   ```

   racadm config -g cfgActiveDirectory -o
   cfgADRacName <nombre común de RAC>

   ```
   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nombre completo del dominio del RAC>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   NOTA: Es necesario configurar al menos una de las tres direcciones. iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. Cuando selecciona la opción de esquema ampliado, éstas son las direcciones IP o el FQDN de los controladores de dominio donde está ubicado el dispositivo iDRAC. Los servidores del catálogo global no se utilizan en el modo de esquema ampliado.

   NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.

PRECAUCIÓN: En esta versión, las funciones de autenticación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el esquema ampliado.

Si desea desactivar la validación de certificados durante el protocolo de enlace SSL, escriba el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

En este caso, no tiene que cargar un certificado de CA.

Si desea aplicar la validación de certificados durante el protocolo de enlace SSL, escriba el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, deberá cargar un certificado de CA con el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

```
racadm sslcertupload -t 0x2 -f <certificado raíz de CA de ADS>
```

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando RACADM:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. Si el DHCP está deshabilitado en el iDRAC o si desea introducir manualmente las direcciones IP de DNS, escriba los siguientes comandos RACADM:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
   ```

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP del DNS primario>
   ```

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP del DNS secundario>
   ```

4. Si desea configurar una lista de dominios de usuario para introducir el nombre de usuario sólo cuando se inicia sesión en la interfaz web del iDRAC6, escriba el siguiente comando:

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <índice>
   ```

   Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

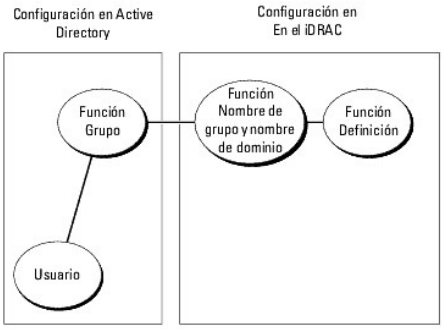
   Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

5. Presione **Entrar** para completar la configuración de Active Directory con esquema ampliado.

Generalidades del esquema estándar de Active Directory

Como se muestra en la Figura 7-3, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en el iDRAC6.

Figura 7-3. Configuración del iDRAC con Microsoft Active Directory y el esquema estándar



En Active Directory, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso al iDRAC6 será miembro del grupo de funciones. Para dar acceso a tales usuarios a un iDRAC6 específico, el nombre del grupo de funciones y el nombre de dominio del mismo deberán estar configurados en el iDRAC6 específico. A diferencia de la solución de esquema ampliado, la función y el nivel de privilegios se definen en cada iDRAC6 y no en Active Directory. Se pueden configurar y definir hasta cinco grupos de funciones en cada iDRAC. La Tabla 7-9 muestra los privilegios predeterminados del grupo de funciones.

Tabla 7-9. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel predeterminado de privilegios	Permisos concedidos	Máscara de bits
Grupo de funciones 1	Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.	0x000001ff
Grupo de funciones 2	Operador:	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC, Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas, Ejecutar comandos de diagnóstico**	0x000000f9
Grupo de funciones 3	Sólo lectura	Inicio de sesión en iDRAC	0x00000001
Grupo de funciones 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de funciones 5	Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios y los grupos de funciones conectados, así como los grupos anidados, están en el mismo dominio, deben configurarse en el iDRAC6 sólo las direcciones de dominio de los controladores. En este caso de dominio único, se admiten todos los tipos de grupos.

Si todos los usuarios y los grupos de funciones conectados, o cualquiera de los grupos anidados, son de múltiples dominios, deben configurarse en el iDRAC6 las direcciones del servidor de catálogo global. En este caso de dominio múltiple, todos los grupos de función y grupos anidados, si los hubiera, deben ser del tipo Grupo universal.

Configuración de Active Directory de esquema estándar para acceder al iDRAC

Debe realizar los pasos siguientes para configurar Active Directory antes de que los usuarios de Active Directory puedan acceder al iDRAC6:

1. En un servidor de Active Directory (controlador de dominio), abra el **complemento de usuarios y equipos de Active Directory.**
2. Cree un grupo o seleccione un grupo existente. Los nombres del grupo y de este dominio deben configurarse en el iDRAC6 por medio de la interfaz web o por medio de RACADM (consulte "Configurar Active Directory con esquema estándar con la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema estándar vía RACADM").
3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para que pueda tener acceso al iDRAC.

Configurar Active Directory con esquema estándar con la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
4. Haga clic en la lengüeta **Configuración** y seleccione **Active Directory**.
5. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparecerá la página **Paso 1 de 4** de **Configuración y administración de Active Directory**.
6. En **Configuración de certificados**, marque **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9**.**
7. En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado.

   NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.
8. Haga clic en **Cargar**.

   Aparecerá la información del certificado de CA de Active Directory válido.
9. En **Cargar Kerberos Keytab**, escriba la ruta de acceso del archivo keytab o bien explore el sistema para localizarlo. Haga clic en **Cargar**. El archivo keytab de Kerberos se cargará en el iDRAC6.
10. Haga clic en **Siguiente** para ir al **Paso 2 de 4** de **Configuración y administración de Active Directory**.
11. Seleccione la opción **Activar Active Directory**.
12. Seleccione la opción **Activar inicio de sesión único** si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autenticación de usuario de dominio, como por ejemplo un nombre de usuario y contraseña.
13. Haga clic en **Agregar** para introducir el nombre de dominio de usuario.
14. Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**.
15. Escriba el **Tiempo de expiración** en segundos para especificar el tiempo que el iDRAC6 tendrá que esperar para las respuestas de Active Directory. El valor predeterminado es 120 segundos.
16. Escriba la dirección de servidor del controlador de dominio. Puede introducir hasta tres servidores Active Directory para procesar los inicios de sesión, pero es necesario que configure al menos un servidor. Para hacerlo, introduzca la dirección IP o el FQDN. iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.
17. Haga clic en **Siguiente** para ir al **Paso 3 de 4** de **Configuración y administración de Active Directory**.
18. En **Selección del esquema**, haga clic en **Esquema estándar.**
19. Haga clic en **Siguiente** para ir al **Paso 4a de 4** de **Configuración y administración de Active Directory.**
20. En **Configuración de esquema estándar**, escriba la dirección del servidor del catálogo global para especificar su ubicación en Active Directory. Debe configurar la ubicación de al menos un servidor del catálogo global.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.

    NOTA: El servidor del catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. En el caso de este dominio múltiple, sólo se puede utilizar el grupo universal.
21. En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

    Aparecerá la página **Paso 4b de 4**.
22. Especifique el **Nombre del grupo de funciones**.

    El **Nombre del grupo de funciones** identifica el grupo de funciones en Active Directory relacionado con el iDRAC.

23. Especifique el **Dominio del grupo de funciones**.

24. Especifique los **Privilegios del grupo de funciones** seleccionando el **Nivel de privilegio del grupo de funciones**. Por ejemplo, si selecciona **Administrador**, se seleccionan todos los privilegios para dicho nivel de permiso.

25. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.

    El servidor web del iDRAC6 regresa automáticamente a la página **Paso 4a de 4 Configuración y administración de Active Directory donde se visualizan sus configuraciones.**

26. Para configurar grupos de funciones adicionales, repita los pasos paso 20 a paso 25.

27. Haga clic en **Finalizar** para regresar a la página **Configuración y administración de Active Directory.**

28. Haga clic en **Probar configuración** para controlar la configuración del esquema estándar de Active Directory.

29. Escriba su nombre de usuario y contraseña de iDRAC6.

    Visualizará los resultados de la prueba y el registro de la misma. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Haga clic en **Acceso remoto→ Configuración→ Red** para configurar los servidores DNS de forma manual o bien utilice DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema estándar.

Configuración de Active Directory con esquema estándar vía RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC con esquema estándar por medio de la interfaz de línea de comandos de RACADM, en lugar de hacerlo mediante la interfaz web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 2
   ```

   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupName <nombre común del grupo de funciones>

   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupDomain <nombre de dominio completo>

   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupPrivilege <Número de máscara de bits para
   permisos de usuarios específicos>

   NOTA: Para obtener los valores del número de máscara de bits, consulte la Tabla B-2.

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>

   NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.

   NOTA: Introduzca el FQDN del controlador de dominio, y *no* sólo el FQDN del dominio. Por ejemplo, introduzca `nombredeservidor.dell.com` en lugar de `dell.com`.

   NOTA: Es necesario configurar al menos una de las 3 direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nombre de dominio completo o dirección IP del controlador de dominio>

   NOTA: El servidor del catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. En el caso de este dominio múltiple, sólo se puede utilizar el grupo universal.

   NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificados.

   Si desea desactivar la validación de certificados durante el protocolo de enlace SSL, escriba el siguiente comando de RACADM:

racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0

En este caso, no es necesario cargar ningún certificado de la autoridad de certificados (CA).

Si desea aplicar la validación de certificados durante el protocolo de enlace SSL, escriba el siguiente comando de RACADM:

racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

racadm sslcertupload -t 0x2 -f <*certificado raíz de CA de ADS*>

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

racadm sslcertdownload -t 0x1 -f <*certificado SSL del RAC*>

2. Si el DHCP está activado en el iDRAC6 y usted desea usar el DNS proporcionado por el servidor DHCP, escriba los siguientes comandos RACADM:

   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1

3. Si el DHCP está desactivado en el iDRAC6 o si usted desea introducir manualmente la dirección IP del DNS, escriba los siguientes comandos de RACADM:

   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <*dirección IP del DNS primario*>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <*dirección IP del DNS secundario*>

4. Si desea configurar una lista de dominios de usuario para introducir el nombre de usuario sólo cuando se inicia sesión en la interfaz web, escriba el siguiente comando:

   racadm config -g cfgUserDomain -o cfgUserDomainName -i <indice>

   Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

   Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

Prueba de las configuraciones realizadas

Si desea verificar si su configuración funciona o si desea diagnosticar el problema en caso de errores al iniciar sesión en Active Directory, puede realizar pruebas de la configuración en la interfaz web del iDRAC6.

Al finalizar la configuración en la interfaz web del iDRAC6, haga clic en **Probar configuración** en la parte inferior de la página. Deberá introducir un nombre de usuario de prueba (por ejemplo, nombredeusuario@dominio.com) y una contraseña para realizar la prueba. Según la configuración, completar todos los pasos de la prueba y mostrar los resultados de cada paso puede tardar un tiempo. Aparecerá un registro detallado de la prueba en la parte inferior de la página de resultados.

Si se produce un error en cualquiera de los pasos, observe la información que aparece en el registro de la prueba para identificar el error y su posible solución. Para obtener información sobre los errores más frecuentes, consulte "Preguntas frecuentes acerca de Active Directory."

Si desea efectuar cambios en la configuración, haga clic en la lengüeta **Active Directory** y modifique la configuración según las instrucciones detalladas.

Activación de SSL en un controlador de dominio

Cuando el iDRAC autentica usuarios con un controlador de dominio de Active Directory, inicia una sesión SSL con el controlador de dominio. En este momento, el controlador de dominio debe publicar un certificado firmado por la autoridad de certificados (CA), cuyo certificado raíz se carga en el iDRAC. En otras palabras, para que el iDRAC pueda autenticarse en *cualquier* controlador de dominio —sin importar si es el controlador de dominio raíz o secundario— el controlador de dominio debe tener un certificado habilitado con SSL firmado por la CA del dominio.

Si va a usar la entidad emisora de certificados raíz de Microsoft para asignar *automáticamente* todos los controladores de dominio a un certificado SSL, realice los pasos siguientes para activar el SSL en cada controlador de dominio:

1. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Política de seguridad del dominio**.
   b. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del ratón en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   c. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y luego en **Finalizar**.

Exportación del certificado de CA del controlador de dominio raíz a iDRAC

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si está utilizando una CA independiente, los siguientes pasos pueden presentar diferencias.

1. Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **Inicio**→ **Ejecutar**.
3. En el campo **Ejecutar**, escriba `mmc` y haga clic en **Aceptar**.
4. En la ventana **Consola 1** (MMC), haga clic en **Archivo (**o **Consola** en sistemas Windows 2000) y seleccione **Agregar/quitar complemento**.
5. En la ventana **Agregar/quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione la **cuenta Equipo** y haga clic en **Siguiente**.
8. Seleccione **Equipo local** y haga clic en **Finalizar**.
9. Haga clic en **Aceptar**.
10. En la ventana **Consola 1,** amplíe la carpeta **Certificados,** amplíe la carpeta **Personal** y haga clic en la carpeta **Certificados**.
11. Localice el certificado de CA raíz y haga clic con el botón derecho en el mismo, seleccione **Todas las tareas** y haga clic en **Exportar...**
12. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
15. Cargue el certificado que guardó en el iDRAC en el paso 14.

    Para cargar el certificado por medio de RACADM, consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema estándar vía RACADM."

    Para cargar el certificado por medio de la interfaz web, consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configurar Active Directory con esquema estándar con la interfaz web del iDRAC6."

Cómo importar el certificado SSL de firmware del iDRAC6

NOTA: Si el servidor de Active Directory está configurado para autenticar el cliente durante una fase de inicialización de sesión SSL, deberá cargar también el certificado de servidor del iDRAC en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de cliente durante la fase de inicialización de una sesión SSL.

Use el siguiente procedimiento para importar el certificado SSL de firmware del iDRAC6 a todas las listas de certificados confiables del controlador de dominio.

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si el certificado SSL de firmware del iDRAC6 está firmado por una CA reconocida y dicho certificado ya se encuentra en la lista de autoridades de certificación de raíz confiables del controlador de dominio, no es necesario realizar los pasos detallados en esta sección.

El certificado SSL de iDRAC es el certificado idéntico que se usa para el servidor web del iDRAC. Todos los controladores del iDRAC se envían con un certificado predeterminado firmado automáticamente.

Para descargar el certificado SSL del iDRAC, ejecute el siguiente comando RACADM:

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

1. En el controlador del dominio, abra una ventana **Consola de MMC** y seleccione **Certificados**→ **Autoridades de certificación de raíz confiables**.
2. Haga clic con el botón derecho del ratón en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
3. Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.
4. Instale el certificado SSL del iDRAC en la lista de **Autoridades de certificación de raíz confiables** de cada controlador de dominio.

   Si ha instalado su propio certificado, asegúrese que la CA que firma su certificado esté en la lista **Autoridad de certificación de raíz confiable**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.

5. Haga clic en **Siguiente** y especifique si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o examine hasta encontrar un almacén de su elección.

6. Haga clic en **Finalizar** y luego en **Aceptar**.

Uso de Active Directory para iniciar sesión en el iDRAC6

Puede utilizar Active Directory para iniciar sesión en el iDRAC6 mediante uno de los siguientes métodos:

- Interfaz web
- RACADM remota
- Consola serie o Telnet

La sintaxis de inicio de sesión la misma para los tres métodos:

<nombre_de_usuario@dominio>

O bien:

*<dominio>**<nombre_de_usuario>* o *<dominio>*/*<nombre_de_usuario>*

donde *nombre_de_usuario* es una cadena ASCII de 1 a 256 bytes.

No se permite usar espacios en blanco ni caracteres especiales (como \, / ó @) en el nombre de usuario ni en el nombre de dominio.

NOTA: No se pueden especificar nombres de dominio NetBIOS, como "América", porque estos nombres no se pueden resolver.

Si inicia sesión en la interfaz web y ha configurado dominios de usuario, la página de inicio de sesión de la interfaz web brindará un menú desplegable de todos los dominios de usuario para que seleccione el deseado. Si selecciona un dominio de usuario del menú desplegable, sólo debe introducir el nombre de usuario. Aun si selecciona **Este iDRAC**, podrá iniciar sesión como usuario de Active Directory si utiliza la sintaxis de inicio de sesión descrita anteriormente en "Uso de Active Directory para iniciar sesión en el iDRAC6."

También puede iniciar en el iDRAC6 por medio de la tarjeta inteligente. Para obtener más información, consulte "Inicio de sesión en el iDRAC6 por medio de la tarjeta inteligente".

NOTA: El servidor de Windows 2008 Active Directory admite sólo una cadena de <nombre_de usuario>@<nombre_de_dominio> con un máximo de 250 caracteres.

Uso del inicio de sesión único de Active Directory

Puede configurar el iDRAC6 para utilizar el protocolo de autenticación de red Kerberos a fin de activar el inicio de sesión único. Para obtener más información sobre cómo configurar el iDRAC6 para usar esta función, consulte "Activación de la autenticación con Kerberos".

Configuración del iDRAC6 para usar el inicio de sesión único

1. Haga clic en **Acceso remoto**→ lengüeta **Configuración**→ sublengüeta **Active Directory**→ y seleccione **Configurar Active Directory**.

2. En la página **Paso 2 de 4 de Configuración y administración de Active Directory**, seleccione **Activar el inicio de sesión único**. La opción **Activar el inicio de sesión único** sólo se habilita si está seleccionada la opción **Activar Active Directory**.

   La opción **Activar el inicio de sesión único** permite iniciar sesión en el iDRAC6 directamente después de conectar la estación de trabajo sin necesidad de introducir credenciales de autenticación de usuario de dominio, como por ejemplo un nombre de usuario y contraseña. Para iniciar sesión en el iDRAC6 por medio de esta función, es necesario haber iniciado sesión en el sistema por medio de una cuenta de usuario de Active Directory válida. Además, también se requiere haber configurado la cuenta de usuario para iniciar sesión en el iDRAC6 por medio de las credenciales de Active Directory. El iDRAC6 utiliza las credenciales de Active Directory guardadas en la caché para permitir el inicio de sesión.

   Para activar la función de inicio de sesión único por medio de la interfaz de línea de comandos, ejecute el siguiente comando racadm:

   ```
   racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
   ```

Inicio de sesión en el iDRAC6 mediante inicio de sesión único

1. Inicie sesión en su estación de trabajo por medio de su cuenta de red.

2. Para acceder a la página web del iDRAC6, escriba los siguientes datos:

   https://*<dirección IP>*

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

https://<*dirección IP*>:<*número de puerto*>

donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

Se abrirá la página de inicio de sesión único del iDRAC6.

3. Haga clic en **Iniciar sesión**.

El iDRAC6 iniciará su sesión por medio de las credenciales que fueron almacenadas en caché en el sistema operativo cuando inició sesión con una cuenta válida de Active Directory.

Preguntas frecuentes acerca de Active Directory

Mi inicio de sesión en Active Directory falló, ¿cómo puedo solucionar este problema?

iDRAC6 proporciona una herramienta de diagnóstico desde la interfaz web. Inicie sesión como usuario local con privilegios de administrador en la interfaz web. Haga clic en **Acceso remoto→ Configuración→ Active Directory**. Desplácese hasta la parte inferior de la página **Configuración y administración de Active Directory**, y haga clic en **Probar configuración**. Introduzca un nombre de usuario y una contraseña de prueba y luego haga clic en **Iniciar prueba**. iDRAC6 ejecuta la prueba paso a paso y muestra el resultado de cada paso. También se registra un resultado detallado de prueba para ayudarlo a resolver los problemas. Haga clic en la lengüeta **Active Directory** para regresar a la página **Configuración y administración de Active Directory**. Desplácese hasta la parte inferior de la página y haga clic en **Configurar Active Directory** para cambiar su configuración y ejecute la prueba nuevamente hasta que el usuario de prueba pase el paso de autorización.

Activé la validación de certificados, pero no puedo iniciar sesión en Active Directory. Ejecuté los diagnósticos de la interfaz gráfica del usuario y los resultados de la prueba muestran el siguiente mensaje de error:

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.

(ERROR: No se puede establecer conexión con el servidor LDAP, error:14090086:SSL rutinas:SSL3_GET_SERVER_CERTIFICATE:error en la validación de certificados: verifique que se haya cargado en el iDRAC el certificado correcto de la autoridad de certificados (CA). Verifique también si la fecha del iDRAC se encuentra dentro del período válido de los certificados y si la dirección del controlador de dominio configurada en el iDRAC concuerda con el sujeto del certificado del servidor de Active Directory.)

¿Cuál puede ser el problema y cómo puedo solucionarlo?

Si la validación de certificados está activada, el iDRAC6 utiliza el certificado de CA cargado para verificar el certificado del servidor de directorio cuando el iDRAC6 establece la conexión SSL con el servidor de directorio. Los motivos más frecuentes de error en la validación de certificados son:

1. La fecha del iDRAC6 no se encuentra dentro del período válido del certificado del servidor o del certificado de CA. Verifique el tiempo del iDRAC6 y el período válido de su certificado.

2. Las direcciones del controlador de dominio configuradas en el iDRAC6 no concuerdan con el sujeto o con el nombre alternativo del sujeto del certificado del servidor de directorio. Si utiliza una dirección IP, lea la siguiente pregunta y respuesta. Si utiliza FQDN, asegúrese de que utiliza el FQDN del controlador de dominio, no el dominio, por ejemplo, nombredeservidor.ejemplo.com en lugar de ejemplo.com.

Estoy usando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?

Verifique el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Generalmente, Active Directory utiliza el nombre de host, no la dirección IP, del controlador de dominio en el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Puede solucionar el problema de diferentes maneras:

1. Configure el nombre del host (FQDN) del controlador de dominio como las *direcciones de controlador de dominio* en el iDRAC6 para que coincidan con el Sujeto o el Nombre alternativo de sujeto del certificado del servidor.

2. Vuelva a emitir el certificado del servidor de forma tal que use una dirección IP en el campo Sujeto o Nombre alternativo de sujeto que concuerde con la dirección IP configurada en el iDRAC6.

3. Desactive la validación de certificados si prefiere confiar en este controlador de dominio sin validación de certificados durante el protocolo de enlace SSL.

Utilizo un esquema ampliado en un entorno de múltiples dominios, ¿cómo debo configurar las direcciones del controlador de dominio?

Debe usar el nombre del host (FQDN) o la dirección IP de los controladores de dominio donde reside el objeto iDRAC6.

¿Cuándo necesito configurar una dirección de catálogo global?

Si utiliza un esquema ampliado, no se utiliza la dirección de catálogo global.

Si está utilizando un esquema estándar, y los usuarios y grupos de funciones pertenecen a dominios distintos, debe configurar las direcciones de catálogo global. En este caso, sólo puede utilizar el grupo universal.

Si está utilizando un esquema estándar, y todos los usuarios y grupos de funciones se encuentran en el mismo dominio, no son necesarias las direcciones de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

iDRAC6 primero se conecta a las direcciones del controlador de dominio configuradas; si el usuario y los grupos de funciones están en el dominio, se guardarán los privilegios.

Si se configuran direcciones de controlador global, el iDRAC6 continúa consultando el catálogo global. Si se recuperan privilegios adicionales del catálogo global, estos privilegios se acumularán.

¿El iDRAC6 siempre usa LDAP a través de SSL?

Sí Todo el transporte se realiza mediante el puerto seguro 636 ó 3269.

Durante la *configuración de prueba*, el iDRAC6 efectúa una CONEXIÓN A LDAP sólo para ayudar a aislar el problema, pero no se vincula a LDAP con una conexión insegura.

¿Por qué el iDRAC6 activa la validación de certificados de forma predeterminada?

El iDRAC6 aplica fuertes medidas de seguridad para asegurar la identidad del controlador de dominio al que se conecta el iDRAC6. Sin la validación de certificados, un pirata informático podría falsificar un controlador de dominio y controlar la conexión SSL. Si decide confiar en todos los controladores de dominio en su barrera de seguridad sin la validación de certificados, puede desactivarla por medio de la interfaz gráfica del usuario o la interfaz de línea de comandos.

¿Es el iDRAC6 compatible con el nombre NetBIOS?

No en esta versión.

¿Qué elementos debo verificar si no puedo iniciar sesión en el iDRAC6 con Active Directory?

Puede diagnosticar el problema haciendo clic en Probar configuración en la parte inferior de la página Configuración y administración de Active Directory en la interfaz web del iDRAC6. Luego, puede solucionar el problema detallado en el resultado de la prueba. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

La mayoría de los problemas se explican en esta sección; sin embargo, por lo general debe verificar lo siguiente:

1. Asegúrese de usar el nombre de dominio de usuario correcto durante un inicio de sesión y no el nombre de NetBIOS.

2. Si tiene una cuenta de usuario local de iDRAC6, inicie sesión en el iDRAC6 usando las credenciales locales.

   Después de haber iniciado sesión:

   a. Asegúrese de haber marcado la casilla **Activar Active Directory** en la página **Configuración de Active Directory** del iDRAC6.

   b. Asegúrese de que la configuración del DNS sea correcta en la página Configuración de la red del iDRAC6.

   c. Asegúrese de que haya cargado el certificado correcto de CA de raíz de Active Directory en el iDRAC6 si activó la validación de certificados. Asegúrese de que el tiempo del iDRAC6 se encuentre dentro del período de validez del certificado de CA.

   d. Si está utilizando el esquema ampliado, asegúrese de que el **Nombre del i**DRAC6 y el **Nombre de dominio del i**DRAC6 coincidan con la configuración del entorno de Active Directory.

      Si está utilizando el esquema estándar, asegúrese de que el **Nombre del grupo** y el **Nombre del dominio del grupo** coincidan con la configuración del entorno de Active Directory.

3. Verifique los certificados de controlador de dominio SSL para asegurarse de que el tiempo del iDRAC6 está dentro del plazo de vigencia del certificado.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la autenticación de tarjeta inteligente

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

El iDRAC6 admite la función de autenticación de dos factores (TFA) si se activa el **Inicio de sesión con tarjeta inteligente**.

Los esquemas tradicionales de autenticación usan nombres de usuario y contraseñas para autenticar a los usuarios. Esto proporciona una seguridad mínima.

En cambio, la función TFA brinda un mayor nivel de seguridad porque los usuarios deben proporcionar dos factores de autenticación, el que poseen y el que conocen. El factor que se posee es la tarjeta inteligente, un dispositivo físico; el factor que se conoce es un código secreto, como una contraseña o PIN.

La autenticación de dos factores requiere que los usuarios verifiquen su identidad al proporcionar *ambos* factores.

Configuración del inicio de sesión con tarjeta inteligente en el iDRAC6

Para activar la función de inicio de sesión con tarjeta inteligente en iDRAC6 desde la interfaz web, diríjase a **Acceso remoto**→ **Configuración**→ **Tarjeta inteligente y seleccione Activar**.

Si usted:

- **Activa** o **Activa con racadm remoto**, se le solicitarán datos de inicio de sesión con tarjeta inteligente en cada intento de inicio de sesión subsiguiente a través de la interfaz web.

  Cuando selecciona **Activar**, todas las interfaces fuera de banda de la interfaz de línea de comandos (CLI), como telnet, SSH, serie, RACADM remota y IPMI en LAN, están desactivadas porque estos servicios solo admiten autenticación de un solo factor.

  Cuando seleccione **Activar con racadm remota**, se desactivarán todas las interfaces fuera de banda de CLI, salvo RACADM remota.

  NOTA: Dell recomienda que el administrador del iDRAC6 utilice la opción **Activar con racadm remota** únicamente para acceder a la interfaz web del iDRAC6 a fin de ejecutar secuencias de comandos por medio de los comandos de RACADM remota. Si el administrador no necesita usar RACADM remota, Dell recomienda que se utilice la opción **Activar** para el inicio de sesión con tarjeta inteligente. Asimismo, compruebe que la configuración de usuario local del iDRAC6 y/o la configuración de Active Directory estén completas antes de activar el **Inicio de sesión con tarjeta inteligente**.

- **Desactivar** la configuración de la tarjeta inteligente (predeterminado). Esta selección desactiva la característica de inicio de sesión con tarjeta inteligente TFA y la siguiente vez que inicia sesión en la interfaz gráfica del iDRAC6, se le pedirá un nombre de usuario y una contraseña de Microsoft® Active Directory® o de sesión local, que es el cuadro de diálogo predeterminado para iniciar sesión en la interfaz web.
- **Activar comprobación de CRL para el inicio de sesión con tarjeta inteligente**: el certificado del iDRAC del usuario, que se descarga del servidor de distribución de la lista de revocación de certificados (CRL) se revisa en la CRL para determinar si se ha revocado.

  NOTA: Los servidores de distribución de CRL aparecen en los certificados de tarjeta inteligente de los usuarios.

Configuración de usuarios de iDRAC6 locales para inicio de sesión con tarjeta inteligente

Puede configurar que los usuarios iDRAC6 locales inicien sesión en el iDRAC6 usando la tarjeta inteligente. Haga clic en **Acceso Remoto**→ **Configuración**→ **Usuarios**.

Sin embargo, antes de que el usuario pueda iniciar sesión en el iDRAC6 con la tarjeta inteligente, usted debe cargar el certificado de tarjeta inteligente del usuario y el certificado de la CA (autoridad de certificados) de confianza para certificar el iDRAC6.

Exportación del certificado de tarjeta inteligente

Puede obtener el certificado del usuario mediante la exportación del certificado de tarjeta inteligente por medio del software de administración de tarjetas (CMS), de la tarjeta inteligente a un archivo en el formato codificado Base64. Habitualmente, el CMS puede obtenerse del proveedor de la tarjeta inteligente. Este archivo codificado se debe cargar como certificado del usuario en el iDRAC6. La autoridad de certificados de confianza que emite los certificados de usuario de tarjeta inteligente también deberá exportar el certificado de CA a un archivo en formato codificado Base64. Debe cargar este archivo como certificado de CA de confianza del usuario. Configure el usuario con un nombre de usuario que forme el nombre principal de usuario (UPN) en el certificado de la tarjeta inteligente.

NOTA: Para iniciar sesión en el iDRAC6, el nombre de usuario que configuró en el iDRAC6 debe ser exactamente igual que el nombre principal de usuario (UPN) que figura en el certificado de tarjeta inteligente.

Por ejemplo, en caso que se haya emitido el certificado de tarjeta inteligente para el usuario, "usuario_muestra@domino.com", el nombre de usuario deberá

configurarse como "usuario_muestra".

Configuración de usuarios de Active Directory para inicio de sesión con tarjeta inteligente

Para configurar los usuarios de Active Directory para que inicien sesión en el iDRAC6 por medio de la tarjeta inteligente, el administrador del iDRAC6 deberá configurar el servidor DNS, cargar el certificado de CA de Active Directory en el iDRAC6 y activar el inicio de sesión de Active Directory. Consulte "Uso del iDRAC6 con Microsoft Active Directory" para obtener más información sobre cómo configurar usuarios de Active Directory.

NOTA: Si el usuario de la tarjeta inteligente está presente en Active Directory, se requiere una contraseña de Active Directory junto con el PIN de la tarjeta inteligente.

Puede configurar Active Directory a partir del menú **Acceso remoto**→ **Configuración**→ **Active Directory**.

Configuración de la tarjeta inteligente

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y después haga clic en **Tarjeta inteligente**.
3. Configure los valores de inicio de sesión con tarjeta inteligente.

   La Tabla 8-1 contiene información sobre los valores de la página **Tarjeta inteligente**.
4. Haga clic en **Aplicar cambios**.

Tabla 8-1. Valores de la tarjeta inteligente

Valor	Descripción
Configurar inicio de sesión con tarjeta inteligente	• **Desactivado**: desactiva el inicio de sesión con tarjeta inteligente. Los inicios de sesión subsiguientes en la interfaz gráfica de usuario mostrarán la página normal de inicio de sesión. Todas las interfaces de línea de comandos fuera de banda, incluso Secure Shell (SSH), Telnet, serie y RACADM remota, toman el valor predeterminado correspondiente. • **Activado**: activa el inicio de sesión con tarjeta inteligente. Después de aplicar los cambios, cierre sesión, inserte su tarjeta inteligente y haga clic en **Iniciar sesión** para introducir el PIN de la tarjeta inteligente. La activación del inicio de sesión con tarjeta inteligente desactiva todas las interfaces fuera de banda de CLI, incluso SSH, Telnet, serie, RACADM remota e IPMI mediante LAN. • **Activado con racadm remoto**: activa el inicio de sesión con tarjeta inteligente junto con RACADM remoto. Todas las demás interfaces fuera de banda de la CLI se desactivan. **NOTA:** El inicio de sesión con tarjeta inteligente requiere que se configuren los usuarios locales del iDRAC6 con los certificados correspondientes. Si se utiliza el inicio de sesión con tarjeta inteligente para que un usuario de Microsoft Active Directory inicie sesión, usted deberá asegurarse de configurar el certificado de usuario de Active Directory para dicho usuario. Puede configurar el certificado de usuario en la página **Usuarios**→**Menú principal de usuario**.
Activar comprobación de CRL para el inicio de sesión con tarjeta inteligente	Esta comprobación sólo está disponible para los usuarios locales de tarjeta inteligente. Seleccione esta opción si desea que el iDRAC6 revise la lista de revocación de certificados (CRL) para ver si el certificado de tarjeta inteligente del usuario ha sido revocado. Para que la función de CRL funcione, el iDRAC6 debe tener una dirección IP de DNS válida establecida como parte de la configuración de la red. Puede configurar la dirección IP de DNS en el iDRAC6: **Acceso remoto**→ **Configuración**→ **Red**. El usuario no podrá iniciar sesión si: • El certificado de usuario aparece revocado en el archivo de CRL. • El iDRAC6 no se puede comunicar con el servidor de distribución de CRL. • El iDRAC6 no puede descargar la CRL. **NOTA:** Debe configurar correctamente la dirección IP del servidor DNS en la página **Configuración**→ **Red** para que esta comprobación se realice correctamente.

Inicio de sesión en el iDRAC6 por medio de la tarjeta inteligente

La interfaz web del iDRAC6 muestra la página de inicio de sesión con tarjeta inteligente de todos los usuario que fueron configurados para usar la tarjeta inteligente.

NOTA: Compruebe que la configuración de usuario local del iDRAC6 y/o la configuración de Active Directory esté completa antes de activar el inicio de sesión con tarjeta inteligente para el usuario.

NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

1. Ingrese a la página web del iDRAC6 usando https.

   https://<*dirección IP*>

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<*dirección IP*>:<*número de puerto*>

   donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

   La página Inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.

   El iDRAC6 solicitará el PIN de la tarjeta inteligente.

3. Introduzca el PIN de la tarjeta inteligente para los usuarios locales de la tarjeta inteligente, y si el usuario no fue creado localmente, el iDRAC6 solicitará que se introduzca la contraseña para la cuenta del usuario en Active Directory.

NOTA: Si usted es un usuario de Active Directory para quien se ha seleccionado la opción **Activar comprobación de CRL para inicio de sesión con tarjeta inteligente**, el iDRAC6 intentará descargar la CRL y buscará en ella el certificado del usuario. El inicio de sesión por medio de Active Directory fallará si el certificado aparece como revocado en la CRL o si la CRL no se puede descargar por cualquier motivo.

Ahora está conectado al iDRAC6.

Inicio de sesión en el iDRAC6 mediante la autenticación con tarjeta inteligente de Active Directory

1. Inicie sesión en el iDRAC6 usando https.

   https://<*dirección IP*>

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<*dirección IP*>:<*número de puerto*>

   donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

   La página Inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.

   Se abrirá el cuadro de diálogo emergente para introducir el PIN.

3. Introduzca el PIN y haga clic en **Aceptar**.

4. Introduzca la contraseña de Active Directory del usuario para autenticar la tarjeta inteligente y haga clic en **Aceptar**.

   De esta forma habrá iniciado sesión en el iDRAC6 con sus credenciales, tal como están definidas en Active Directory.

NOTA: Si el usuario de la tarjeta inteligente está presente en Active Directory, se requiere una contraseña de Active Directory junto con el PIN de la tarjeta inteligente. En versiones futuras, es posible que no se requiera la contraseña de Active Directory.

Solución de problemas de inicio de sesión con la tarjeta inteligente en el iDRAC6

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Compruebe que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows®. Windows admite una cantidad limitada de proveedores de servicios criptográficos (CSP) de tarjetas inteligentes.

Consejo: como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y revise si Windows detecta la tarjeta inteligente y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

Imposible iniciar sesión en el iDRAC6 local

Si un usuario del iDRAC6 local no puede iniciar sesión, revise si el nombre de usuario y los certificados de usuario que están cargados en el iDRAC6 han expirado. Los registros de rastreo del iDRAC6 pueden proporcionar mensajes importantes de registro relacionados con errores; sin embargo, los mensajes de error son, algunas veces, intencionalmente ambiguos por motivos de seguridad.

No se puede iniciar sesión en el iDRAC6 como usuario de Active Directory

Si no puede iniciar sesión en el iDRAC6 como usuario de Active Directory, trate de iniciar sesión en el iDRAC6 sin activar el inicio de sesión con tarjeta inteligente. Si ha activado la comprobación de CRL, intente iniciar sesión en Active Directory sin activar la comprobación de CRL. El registro de rastreo de iDRAC6 deberá proporcionar importantes mensajes si se presenta algún error de CRL.

También tiene la opción de desactivar el inicio de sesión con tarjeta inteligente a través de racadm local con el siguiente comando:

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la redirección de consola con interfaz gráfica de usuario

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección proporciona información acerca de cómo usar la función de redirección de consola del iDRAC6.

Información general

La función de redirección de consola del iDRAC6 le permite tener acceso a la consola del servidor local de manera remota en modo gráficos o de texto. Por medio de la redirección de consola, puede controlar uno o varios sistemas equipados con iDRAC6 desde una ubicación.

No es necesario ir personalmente a cada servidor para realizar todo el mantenimiento de rutina. En vez de eso, usted puede administrar los servidores desde donde se encuentre, desde su equipo de escritorio o desde su equipo portátil. También puede compartir la información con otros; de manera remota e instantánea.

Uso de redirección de consola

NOTA: Cuando usted abre una sesión de redirección de consola, el servidor administrado no indica que la consola ha sido redirigida.

NOTA: Si ya hay abierta una sesión de redirección de consola, desde la estación de administración al iDRAC6, al intentar abrir una nueva sesión desde la misma estación de administración a ese iDRAC6, se activará la sesión existente. No se generará una nueva sesión.

NOTA: Es posible abrir varias sesiones de redirección de consola desde una sola estación de administración hacia múltiples controladoras del iDRAC6 simultáneamente.

La página **Redirección de consola** permite administrar el sistema remoto con el teclado, vídeo y ratón en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta característica puede ser usada junto con la característica de medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- Se admite un máximo de cuatro sesiones simultáneas de redirección de consola. Todas las sesiones muestran la misma consola de servidor administrado simultáneamente.
- Sólo se puede abrir una sesión hacia un servidor remoto (iDRAC6) desde la misma consola cliente (estación de administración). Sin embargo, se pueden abrir varias sesiones hacia varios servidores remotos desde el mismo cliente.
- La sesión de redirección de consola no se deberá ejecutar desde un explorador web en el sistema administrado.
- Se requiere un ancho de banda disponible de red de al menos 1 MB/s.

La primera sesión de redirección de consola hacia el iDRAC es una sesión de acceso completo. Si otro usuario solicita una sesión de redirección de consola, el primer usuario recibe una notificación y tiene la opción de rechazarla, **permitirla como sólo lectura** o **aprobarla**. El segundo usuario es notificado de que otro usuario tiene el control. El primer usuario debe responder en treinta segundos o se rechazará el acceso al segundo usuario.

Todas las sesiones **permitidas como sólo lectura** se cierran automáticamente cuando finaliza la última sesión que tiene acceso completo.

Configuración de la estación de administración

Para usar la redirección de consola en la estación de administración, realice los siguientes procedimientos:

1. Instale y configure un explorador web admitido. Consulte las siguientes secciones para obtener más información:
   - "Exploradores web admitidos"
   - "Configuración de un explorador web admitido"

   NOTA: Debe instalarse Java Runtime Environment en la estación de administración para que funcione la función de redirección de consola.

2. Si utiliza Internet Explorer, asegúrese de que el explorador esté activado para descargar contenido cifrado de esta forma:
   - Desde Internet Explorer, vaya a Opciones o Configuración y seleccione **Herramientas**→ **Opciones de Internet**→ **Opciones avanzadas**.
   - Desplácese hasta la sección **Seguridad** y desmarque esta opción:

     Do not save encrypted pages to disk (No guardar las páginas cifradas en el disco.)

3. Se recomienda que configure la resolución del monitor en 1280 x 1024 pixeles o más.

NOTA: Si el sistema ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el KVM del iDRAC, se cambiará de Linux a consola de texto.

NOTA: Ocasionalmente, puede encontrar el siguiente error de compilación de Java Script: "Expected: ; ("Esperado: ;"). Para resolver este problema, ajuste la configuración de la red para utilizar la "Conexión directa" en JavaWebStart: "Editar->Preferencias->General->Configuración de red" y elija "Conexión directa" en lugar de "Utilizar configuración del explorador".

Configuración de la redirección de consolaen la interfaz web del iDRAC6

Para configurar la redirección de consola en la interfaz web del iDRAC6, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **Consola / Medios**→ **Configuración** para configurar los ajustes de redirección de consola del iDRAC.
2. Configure las propiedades de la redirección de consola. La Tabla 10-1 describe la configuración de la redirección de consola.
3. Cuando termine, haga clic en **Aplicar cambios**.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 10-2.

Tabla 10-1. Propiedades de configuración de la redirección de consola

Propiedad	Descripción
Activado	Haga clic para activar o desactivar la Redirección de consola. Si esta opción aparece marcada, indica que la redirección de consola está activada. El valor predeterminado es **activado**. **NOTA:** Si la opción **Activado** se marca o deja en blanco después de iniciar el KVM virtual, pueden desconectarse todas las sesiones de KVM virtual existentes.
Máx. de sesiones	Muestra el número máximo posible de sesiones de redirección de consola, 1 a 4. Use el menú desplegable para cambiar el número máximo permitido de sesiones de redirección de consola. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de consola activa. Este campo es de sólo lectura.
Puerto de presencia remota	El número de puerto de red utilizado para conectar a la opción de teclado/ratón de la redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es **5900**. **NOTA:** Si la opción **Puerto de presencia remota** se modifica después de iniciar el KVM virtual, pueden desconectarse todas las sesiones de KVM virtual existentes.
Cifrado de vídeo activado	**Seleccionado** indica que el cifrado de vídeo está activado. Todo el tráfico que se dirige al puerto de vídeo está cifrado. **Deseleccionado** indica que el cifrado de vídeo está desactivado. El tráfico que va al puerto de vídeo no está cifrado. El valor predeterminado es **Cifrado. La desactivación del cifrado puede mejorar el rendimiento en las redes más lentas.** **NOTA:** Si la opción **Cifrado de vídeo activado** se activa o deshabilita después de iniciar el KVM virtual, pueden desconectarse todas las sesiones de KVM virtual existentes.
Vídeo del servidor local activado	Si está seleccionado, indica que la salida al monitor de KVM del iDRAC está desactivada durante la redirección de consola. Esto garantiza que las tareas que realice usando **Redirección de consola** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte "Configuración y uso de medios virtuales".

Los botones que se muestran en la Tabla 10-2 están disponibles en la página **Configuración**.

Tabla 10-2. Botones de la página de configuración

Botón	Definición
Imprimir	Imprime la página
Actualizar	Vuelve a cargar la página **Configuración**
Aplicar cambios	Guarda los ajustes nuevos o modificados

Abrir una sesión de redirección de consola

Al abrir una sesión de redirección de consola, la aplicación Dell™ Virtual KVM Viewer se inicia y en el visor aparece el escritorio del sistema remoto. Al usar la aplicación Virtual KVM Viewer, puede controlar las funciones de ratón y teclado del sistema remoto desde la estación de administración local.

Para abrir una sesión de redirección de consola en la interfaz web, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **Consola / Medios**→ **Redirección de consola y medios virtuales**.

2. Utilice la información de la Tabla 10-3 para asegurarse de que una sesión de redirección de consola está disponible.

   Si desea volver a configurar los valores de propiedades que se muestran, consulte "Configuración de la redirección de consolaen la interfaz web del iDRAC6".

Tabla 10-3. Redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No (seleccionado/no seleccionado)
Cifrado de vídeo activado	Sí/No (seleccionado/no seleccionado)
Máx. de sesiones	Muestra el número máximo de sesiones de redirección de consola admitidas
Sesiones activas	Muestra el número actual de sesiones activas de redirección de consola
Vídeo del servidor local activado	Sí = activado; No = desactivado.
Puerto de presencia remota	El número de puerto de red utilizado para conectar a la opción de teclado/ratón de la redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es 5900.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte "Configuración y uso de medios virtuales".

Los botones en la Tabla 10-4 están disponibles en la página **Redirección de consola y medios virtuales**.

Tabla 10-4. Botones de la página Redirección de consola y medios virtuales

Botón	Definición
Actualizar	Actualiza la página **Redirección de consola y medios virtuales**.
Iniciar el visor	Abre una sesión de redirección de consola en el sistema remoto de destino
Imprimir	Imprime la página **Redirección de consola y medios virtuales**.

3. Si hay una sesión de redirección de consola disponible, haga clic en **Iniciar el visor**.

   NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de los tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

   NOTA: Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información en la ventana y haga clic en **Sí** para seguir.

   La estación de administración se conecta al iDRAC6 y la pantalla de escritorio del sistema remoto aparece en la aplicación iDRAC KVM Viewer.

4. Aparecerán dos punteros de ratón en la ventana del visor: uno para el sistema remoto y otro para el sistema local. Puede cambiar a un solo cursor al seleccionar la opción **Un solo cursor** en **Herramientas** en el menú de KVM del iDRAC.

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver la pantalla de escritorio del servidor administrado y controlar las funciones de ratón y teclado desde la estación de administración. Cuando se conecta con el sistema remoto, Video Viewer se inicia en otra ventana.

NOTA: Si el servidor remoto está apagado, se visualizará el mensaje **No Signal (Sin señal)**.

Video Viewer proporciona varios ajustes de control, por ejemplo, sincronización del ratón, instantáneas, macros de teclado y acceso a los medios virtuales. Para obtener más información sobre estas funciones, haga clic en **Sistema**→ **Consola / Medios** y haga clic en **Ayuda en la página Redirección de consola y medios virtuales**.

Cuando comience una sesión de redirección de consola y aparezca Video Viewer, es posible que deba sincronizar los punteros del ratón.

Desactivación o activación del vídeo del servidor local

Usted puede configurar el iDRAC6 para rechazar conexiones de KVM del iDRAC por medio de la interfaz web del iDRAC6.

Si desea asegurarse de tener acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local *y volver a configurar el* **Máx. de**

sesiones a 1 en la **página Configuración de redirección de consola**.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, no se desactivarán el monitor, teclado y ratón que están conectados al KVM del iDRAC.

Para desactivar o activar la consola local, realice el procedimiento siguiente:

1. En la estación de administración, abra un explorador web admitido e inicie sesión en el iDRAC6. Consulte "Acceso a la interfaz web" para obtener más información.
2. Haga clic en **Sistema**→ **Consola / Medios**→ **Configuración**.
3. Para desactivar (apagar) el vídeo local en el servidor, desmarque la casilla de verificación **Vídeo del servidor local activado** en la página **Configuración**, y luego haga clic en **Aplicar**. El valor predeterminado es Desactivado.

   NOTA: Si el vídeo del servidor local está encendido, demorará 15 segundos en apagarse.

4. Para activar (encender) el vídeo local en el servidor, marque la casilla de verificación **Vídeo del servidor local activado** en la página **Configuración**, y luego haga clic en **Aplicar**.

Preguntas frecuentes sobre la redirección de consola

La Tabla 10-5 contiene las preguntas y respuestas frecuentes.

Tabla 10-5. Uso de la redirección de consola: preguntas frecuentes

Pregunta	Respuesta
¿Se puede iniciar una nueva sesión de vídeo de consola remota cuando el vídeo local del servidor está apagado?	Sí.
¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del vídeo local?	Esto brinda al usuario local la oportunidad de realizar alguna acción antes de que el vídeo se apague.
¿Hay algún retraso al encender el vídeo local?	No. Después de que el iDRAC6 recibe la solicitud de **encendido** de vídeo local, el vídeo se enciende instantáneamente.
¿El usuario local también puede apagar el vídeo?	Cuando la consola local está desactivada, el usuario local no puede apagar el vídeo.
¿El usuario local también puede encender el vídeo?	Cuando la consola local está desactivada, el usuario local no puede encender el vídeo.
¿La desactivación del vídeo local también desactiva el teclado y el ratón locales?	No.
¿La desactivación de la consola local desactivará el vídeo en la sesión de consola remota?	No, la activación o desactivación del vídeo local es independiente de la sesión de consola remota.
¿Cuáles son los privilegios necesarios para que un usuario del iDRAC6 active o desactive el vídeo del servidor local?	Cualquier usuario con privilegios de configuración del iDRAC6 puede activar o desactivar la consola local.
¿Cómo se puede ver el estado actual del vídeo del servidor local?	El estado se muestra en la página **Configuración de redirección de consola** de la interfaz web del iDRAC6. El comando **racadm getconfig –g cfgRacTuning** de la interfaz de línea de comandos de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**.
No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024. Pruebe utilizar las barras de desplazamiento también en el cliente KVM del iDRAC.
La ventana de la consola no es legible.	El visor de la consola en Linux requiere de un conjunto de caracteres UTF-8. Revise la configuración regional y, de ser necesario, restablezca el conjunto de caracteres.
¿Por qué no se sincroniza el ratón en la consola de texto de Linux?	El KVM virtual necesita el controlador de ratón USB, pero el controlador de ratón USB sólo está disponible en el sistema operativo X-Window.
Aún tengo problemas con la sincronización del ratón.	Compruebe que el ratón adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de redirección de consola. Asegúrese de que la opción **Un solo cursor** en **Herramientas** que aparece en el menú de KVM del iDRAC esté seleccionada en el cliente KVM del iDRAC.
¿Por qué no puedo usar un teclado o ratón mientras instalo un sistema operativo de Microsoft® de manera remota mediante la redirección de consola del iDRAC6?	Cuando instala de manera remota un sistema operativo Microsoft admitido en un sistema con la redirección de consola habilitada en el BIOS, aparece un mensaje de conexión de EMS que le pide que seleccione **Aceptar** para poder continuar. Usted no puede usar el ratón para seleccionar **Aceptar** de manera remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la redirección de consola en el BIOS. Microsoft genera este mensaje para avisar al usuario que la redirección de consola está activada. Para asegurar que este mensaje no aparece, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Num de mi estación de administración no muestra el	Cuando se accede por medio del iDRAC6, el indicador Bloq Num de la estación de administración no necesariamente coincide con el estado del Bloq Num del servidor remoto. El estado de Bloq Num depende de la

estado de Bloq Num en el servidor remoto?	configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Num en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una sesión de redirección de consola desde el host local?	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado, ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, ambos tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?	Dell recomienda una conexión de 5 MB/s para un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la redirección de consola?	Se requiere que la estación de administración tenga un procesador Intel® Pentium® III de 500 MHz con 256 MB de RAM como mínimo.
¿Por qué veo un mensaje de **Sin señal** dentro de la aplicación iDRAC KVM Video Viewer?	Es posible que vea este mensaje porque el complemento de iDRAC Virtual KVM no recibe el vídeo del escritorio del servidor remoto. Generalmente, este comportamiento puede ocurrir cuando el servidor remoto está apagado. Ocasionalmente, el mensaje puede aparecer porque ocurrió una falla con la recepción del vídeo del escritorio del servidor remoto.
¿Por qué veo un mensaje de **Fuera de rango** dentro de la aplicación iDRAC KVM Video Viewer?	Es posible que vea este mensaje porque un parámetro necesario para capturar el vídeo esté fuera del rango para el cual el iDRAC puede capturar el vídeo. Los parámetros como la resolución de pantalla o la frecuencia de actualización que estén muy elevados provocarán una condición de fuera de rango. Por lo general, el rango máximo de parámetros se configura por limitaciones físicas como el tamaño de la memoria de vídeo o el ancho de banda.

Regresar a la página de contenido

Regresar a la página de contenido

Activación de la autenticación con Kerberos

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Kerberos es un protocolo de autenticación de red que permite que los sistemas se comuniquen de forma segura a través de una red sin protección. Para ello, los sistemas deben demostrar su autenticidad. Para mantener los más altos estándares de cumplimiento de autenticación, el iDRAC6 ahora admite la autenticación de Active Directory® con Kerberos para permitir el inicio de sesión único y con tarjeta inteligente en Active Directory.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® y Windows Server 2008 utilizan Kerberos como método de autenticación predeterminado.

El iDRAC6 utiliza Kerberos para admitir dos tipos de mecanismos de autenticación: el inicio de sesión único y con tarjeta inteligente en Active Directory. Para el inicio de sesión único, el iDRAC6 emplea las credenciales de usuario almacenadas en caché en el sistema operativo al iniciar sesión mediante una cuenta válida de Active Directory.

Para el inicio de sesión con tarjeta inteligente de Active Directory, el iDRAC6 utiliza la autenticación de dos factores (TFA) con tarjeta inteligente a modo de credenciales para permitir el inicio de sesión en Active Directory. Ésta es la función siguiente a la autenticación con tarjeta inteligente local.

La autenticación de Kerberos en el iDRAC6 fallará si la hora del iDRAC6 difiere de la hora del controlador de dominio. Se permite una diferencia máxima de 5 minutos. Para permitir una autenticación correcta, sincronice la hora del servidor con la hora del controlador de dominio y después **restablezca** el iDRAC6.

También puede utilizar el siguiente comando de diferencia de zona horaria de RACADM para sincronizar la hora:

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <valor de diferencia>
```

Requisitos previos para el inicio de sesión único y la autenticación de Active Directory mediante tarjeta inteligente

- Configure el iDRAC6 para el inicio de sesión de Active Directory. Para obtener más información, consulte "Uso de Active Directory para iniciar sesión en el iDRAC6".
- Registre el iDRAC6 como equipo en el dominio raíz de Active Directory.
  a. Haga clic en **Acceso remoto**→ lengüeta **Configuración**→ sublengüeta **Red**.
  b. Indique una dirección IP de **servidor DNS alternativo / preferido** que sea válida. Este valor señala la dirección IP del servidor DNS que forma parte del dominio raíz, que autentica las cuentas de Active Directory de los usuarios.
  c. Seleccione **Registrar el iDRAC en DNS**.
  d. Brinde un **nombre de dominio DNS** válido.

  Consulte la ***ayuda en línea del iDRAC6*** para obtener información adicional.

Para permitir el uso de los dos nuevos mecanismos de autenticación, el iDRAC6 admite la configuración para activarse como servicio "kerberizado" en una red Windows con Kerberos. La configuración de Kerberos en el iDRAC6 requiere los mismos pasos que la configuración de un servicio Kerberos externo a Windows Server como principal función de seguridad en Windows Server Active Directory.

La herramienta **ktpass** de Microsoft (proporcionada por Microsoft como parte del CD/DVD de instalación del servidor) se utiliza para crear el enlace del nombre principal de servicio (SPN) con una cuenta de usuario y exportar la información de confianza a un archivo *keytab* de Kerberos de tipo MIT, lo que permite establecer una relación de confianza entre un usuario o sistema externo y el centro de distribución de claves (KDC). El archivo keytab contienen una clave criptográfica que se usa para cifrar la información entre el servidor y el KDC. La herramienta ktpass permite el uso de servicios basados en UNIX que admiten la autenticación Kerberos para ejecutar las funciones de interoperabilidad proporcionadas por un servicio Kerberos KDC de Windows Server.

El archivo keytab que se obtiene de la utilidad ktpass está disponible para el iDRAC6 como archivo para cargar y es activado para actuar como un servicio kerberizado en la red.

Como el iDRAC6 es un dispositivo con un sistema operativo que no es Windows, ejecute la utilidad **ktpass** (que es parte de Microsoft Windows) en el controlador de dominio (servidor Active Directory) donde desea asignar el iDRAC6 a una cuenta de usuario de Active Directory.

Por ejemplo, utilice el comando **ktpass** a continuación para crear el archivo keytab de Kerberos:

```
C:\>ktpass -princ HOST/dracname.domainname.com@DOMAINNAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

El tipo de cifrado admitido por el iDRAC6 para la autenticación con Kerberos es DES-CBC-MD5. El tipo principal es KRB5_NT_PRINCIPAL. Las siguientes propiedades de la cuenta de usuario a la que está conectado el nombre principal de servicio deberán estar activadas:

- Usar tipos de cifrado DES para esta cuenta
- No requerir autenticación previa de Kerberos

NOTA: Se recomienda usar la utilidad **ktpass** más reciente para crear el archivo keytab.

Este procedimiento generará un archivo keytab que deberá cargar en el iDRAC6.

NOTA: Este archivo contiene una clave de cifrado y debe mantenerse guardado de manera segura.

Para obtener más información sobre la utilidad **ktpass**, visite el sitio web de Microsoft:
http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

- La hora del iDRAC6 debe sincronizarse con el controlador de dominio de Active Directory.

Configuración del iDRAC6 para el inicio de sesión único y la autenticación de Active Directory mediante tarjeta inteligente

Cargue en el iDRAC6 el archivo keytab obtenido del dominio raíz de Active Directory:

1. Haga clic en **Acceso remoto**→ lengüeta **Configuración**→ sublengüeta **Active Directory**→ y haga clic en **Configurar Active Directory**.
2. Seleccione **Cargar keytab de Kerberos** y haga clic en **Siguiente**.
3. En la página **Cargar keytab de Kerberos**, seleccione el archivo keytab que desea cargar y haga clic en **Aplicar**.

También puede cargar el archivo en el iDRAC6 mediante comandos racadm de la interfaz de línea de comandos. El siguiente comando permite cargar el archivo keytab en iDRAC6:

```
racadm krbkeytabupload -f <nombre_de_archivo>
```

donde <nombre_de_archivo> es el nombre del archivo keytab. El comando racadm es compatible con racadm local y remoto.

Configuración de usuarios de Active Directory para el inicio de sesión único

Antes de usar la función de inicio de sesión único de Active Directory, asegúrese de que el iDRAC6 ya está configurado para el inicio de sesión de Active Directory y de que la cuenta de usuario de dominio que se utilizará para iniciar sesión en el sistema está activada para el inicio de sesión en Active Directory del iDRAC6.

Asimismo, verifique que la configuración de inicio de sesión de Active Directory está activada. Consulte "Uso del iDRAC6 con Microsoft Active Directory" para obtener más información sobre cómo configurar usuarios de Active Directory. El iDRAC6 también debe estar activado para representar un servicio kerberizado. Para ello es necesario cargar en el iDRAC6 un archivo *keytab* válido obtenido del dominio raíz de Active Directory.

Consulte "Configuración del iDRAC6 para usar el inicio de sesión único" para obtener información sobre cómo activar el inicio de sesión único por medio de la interfaz gráfica del usuario (GUI) y la interfaz de línea de comandos (CLI).

Inicio de sesión en el iDRAC6 con la función de inicio de sesión único para usuarios de Active Directory

NOTA: Para conectarse con el iDRAC6, asegúrese de contar con los más recientes componentes de ejecución de las bibliotecas Microsoft Visual C++ 2005. Para obtener más información, consulte el sitio web de Microsoft.

1. Inicie sesión en el sistema por medio de una cuenta de Active Directory válida.
2. Escriba la dirección web del iDRAC6 en la barra de direcciones del explorador.

   NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para inicio de sesión único cuando utiliza esta función por primera vez.

   Usted estará conectado al iDRAC6 con los privilegios adecuados de Microsoft Active Directory si:

   - Es usuario de Microsoft Active Directory.
   - Está configurado en el iDRAC6 para el inicio de sesión de Active Directory.
   - El iDRAC6 está activado para la autenticación de Active Directory con Kerberos.

Configuración de usuarios de Active Directory para inicio de sesión con tarjeta inteligente

Antes de usar la función de inicio de sesión con tarjeta inteligente de Active Directory, asegúrese de que el iDRAC6 ya está configurado para el inicio de sesión

de Active Directory y de que la cuenta de usuario para la que se emitió la tarjeta inteligente está activada para el inicio de sesión en Active Directory del iDRAC6.

Asimismo, verifique que la configuración de inicio de sesión de Active Directory está activada. Consulte "Uso del iDRAC6 con Microsoft Active Directory" para obtener más información sobre cómo configurar usuarios de Active Directory. El iDRAC6 también debe estar activado para representar un servicio kerberizado. Para ello es necesario cargar en el iDRAC6 un archivo *keytab* válido obtenido del dominio raíz de Active Directory.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz WS-MAN

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

El firmware del iDRAC6 ofrece administración de acceso de red mediante el uso del protocolo de servicios web para administración (WS-MAN). WS-MAN es un mecanismo de transporte para intercambio de información. WS-MAN ofrece un idioma universal para que los dispositivos puedan compartir datos, de forma que se puedan administrar más fácilmente. WS-MAN es una parte esencial de una solución de administración de sistemas remotos, aunque no es la única.

WS-MAN usa HTTPS para mantener el tráfico de administración seguro. El cliente debe iniciar sesión mediante el uso de privilegios de usuario local o de Microsoft® Active Directory® para autenticar la sesión. HTTPS usa la capa de sockets seguros (SSL) en el puerto IP 443 para mantener comunicaciones seguras.

Los datos disponibles mediante WS-MAN son un subconjunto de datos proporcionados por la interfaz de instrumentación del iDRAC6 asignada a los siguientes perfiles de grupo de trabajo de administración distribuida (DMTF) y perfiles de extensión de Dell.

El uso de WS-MAN para transmitir información de administración basada en CIM de DMTF es el uso más común de WS-MAN. CIM define los tipos de información de administración que pueden manipularse en un sistema administrado. Ofrece los objetos sobre los que el cliente y el servicio hablan en la conexión. WS-MAN especifica algunas acciones estándar que pueden realizarse en los objetos de administración. Por ejemplo, mediante el uso de WS-MAN, un sistema cliente puede buscar una recopilación de objetos de administración, obtener el contenido de un objeto de administración y establecer su contenido en valores nuevos. WS-MAN ofrece los verbos de la conversación de administración; las propiedades y las clases de CIM son los sustantivos, los objetos sobre los que actúan los verbos.

Para garantizar la interoperabilidad entre los clientes y los servicios, DMTF y Dell también especifican un *vocabulario* mínimo estándar de clases de CIM, propiedades y comportamientos que todas las partes deben comprender. Estos perfiles específicos de DMTF y Dell definen un conjunto de convenciones que todos los servicios que cumplen con los estándares deben implementar. Por lo tanto, todos los clientes pueden depender de estas convenciones para funcionar correctamente.

Perfiles CIM admitidos

Tabla 11-1. Perfiles CIM admitidos

DMTF estándar
1. Servidor básico Define las clases de CIM para representar el servidor host.
2. Procesador de servicio: Contiene la definición de las clases de CIM para representar el iDRAC6. **NOTA:** El perfil básico del servidor (arriba) y el perfil de procesador de servicio son autónomos en el sentido de que los objetos que describen agrupan todos los otros objetos CIM que se definen en los perfiles de componentes.
3. Propiedad física: Define las clases de CIM para representar el aspecto físico de los elementos administrados. El iDRAC6 usa este perfil para representar la información de FRU del servidor host y de sus componentes, además de la tipología física.
4. Admin de dominios SM CLP Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
5. Administración del estado de la alimentación Define las clases de CIM para las operaciones de control de alimentación. El iDRAC6 usa este perfil para las operaciones control de alimentación del servidor host.
6. Suministro de energía (versión 1.1) Define las clases de CIM para representar suministros de energía. El iDRAC6 usa este perfil para representar los suministros de energía del servidor host para describir el consumo de energía, como las marcas de agua de consumo de energía alto y bajo.
7. Servicio CLP Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
8. Interfaz IP
9. Cliente DHCP
10. Cliente DNS
11. Puerto Ethernet Los perfiles anteriores definen las clases de CIM para representar apilamientos de red. El iDRAC6 usa estos perfiles para representar la configuración de la tarjeta de interfaz de red del iDRAC6.
12. Registro Define las clases de CIM para representar distintos tipos de registros. El iDRAC6 usa este perfil para representar el registro de eventos del sistema

(SEL) y el registro RAC del iDRAC6.
13. Inventario de software Define las clases de CIM para inventario de software instalado o disponible. El iDRAC6 usa este perfil para inventario de versiones de firmware del iDRAC6 actualmente instaladas mediante el protocolo TFTP.
14. Autorización basada en funciones Define las clases de CIM para representar funciones. El iDRAC6 usa este perfil para configurar privilegios de la cuenta iDRAC6.
15. Actualización de software Define las clases de CIM para inventario de actualizaciones de software disponibles. El iDRAC6 usa este perfil para inventario de actualizaciones de firmware mediante el protocolo TFTP.
16. Recopilación SMASH Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
17. Registro de perfiles Define las clases de CIM para anunciar las implementaciones de perfil. El iDRAC6 usa este perfil para anunciar sus propios perfiles implementados, como se describe en esta tabla.
18. Medidas básicas Define las clases de CIM para representar las medidas. El iDRAC6 usa este perfil para representar las medidas del servidor host para describir el consumo de energía, como las marcas de agua de consumo de energía alto y bajo.
19. Administración de identidad simple Define las clases de CIM para representar identidades. El iDRAC6 usa este perfil para la configuración de cuentas iDRAC6.
20. Redirección de USB Define las clases de CIM para representar la redirección remota de puertos USB locales. El iDRAC6 usa este perfil junto con el perfil de medios virtuales para configurar medios virtuales.
Extensiones de Dell
1. Dell™ Active Directory Client versión 2.0.0 Define las clases de extensiones de CIM y Dell para configurar el cliente iDRAC6 Active Directory y los privilegios locales para grupos de Active Directory.
2. Medios virtuales de Dell Define las clases de extensiones de CIM y Dell para configurar los medios virtuales del iDRAC6. Extiende el perfil de redirección de USB
3. Puerto Ethernet de Dell Define las clases de extensiones de CIM y Dell para configurar la interfaz NIC Side-Band para la tarjeta de interfaz de red del iDRAC6. Extiende el perfil de puerto Ethernet.
4. Administración de la utilización de la alimentación de Dell Define las clases de extensiones de CIM y Dell para representar el presupuesto de alimentación del servidor host y para configurar/supervisar el presupuesto de alimentación del servidor host.

Para obtener más información, consulte **www.dmtf.org/standards/profiles/**. Para acceder a actualizaciones de esta lista de perfiles u obtener información, consulte las notas sobre la versión de WS-MAN o el archivo léame.

La implementación de WS-MAN cumple con la especificación DMTF WS-MAN versión 1.0.0. Las herramientas compatibles conocidas que admiten el protocolo WS-MAN incluyen (entre otras) las herramientas de Microsoft Windows® Remote Management (WinRM), open wsman y wsmancli.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de SM-CLP del iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección ofrece información acerca del protocolo de línea de comandos para la administración de servidores (SM-CLP) del equipo de trabajo de administración distribuida (DMTF) que está incorporado en el iDRAC6.

NOTA: En esta sección se parte de la premisa de que el lector está familiarizado con la iniciativa SMASH (arquitectura de administración de sistemas para hardware de servidor) y las especificaciones de SM-CLP. Para obtener más información sobre estas especificaciones, visite el sitio web de DMTF en **www.dmtf.org**.

El SM-CLP del iDRAC6 es un protocolo que ofrece estándares para implementaciones de la interfaz de línea de comandos para administración de sistemas. El SM-CLP es un subcomponente de la iniciativa de SMASH supervisado por DMTF para una administración efectiva del servidor en varias plataformas. La especificación SM-CLP, junto con la especificación de direccionamiento de elemento administrado y varios perfiles en las especificaciones de asignación de SM-CLP, describe los destinos y verbos estandarizados para distintas ejecuciones de tareas de administración.

Compatibilidad con SM-CLP de iDRAC6

El SM-CLP se aloja en el firmware del controlador iDRAC6 y admite las interfaces Telnet, SSH y serie. La interfaz de SM-CLP del iDRAC6 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por la organización DMTF. SM-CLP del iDRAC6 admite todos los perfiles que se describen en la Tabla 11-1 "Perfiles CIM admitidos".

Las siguientes secciones proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC6.

Funciones de SM-CLP

El SM-CLP promueve el concepto de verbos y destinos para brindar capacidades de administración de sistemas por medio de la interfaz de línea de comandos. El verbo indica la operación que se va a ejecutar y el destino determina la entidad (u objeto) que ejecuta la operación.

A continuación, se muestra un ejemplo de la sintaxis de la línea de comandos de SM-CLP.

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

Durante una sesión típica de SM-CLP, puede realizar operaciones mediante los verbos que se mencionan en la Tabla 12-1.

Tabla 12-1. Verbos CLI admitidos para el sistema

Verbo	Definición
cd	Navega en el MAP por medio del shell
set	Establece una propiedad para un valor específico
help	Muestra la ayuda de un destino específico
reset	Restablece el destino
show	Muestra las propiedades del destino, los verbos y los destinos secundarios
start	Activa un destino
stop	Desactiva un destino
exit	Cierra la sesión de shell de SM-CLP
version	Muestra los atributos de versión de un destino
load	Lleva una imagen binaria de una URL a una dirección de destino especificada

Uso de SM-CLP

Establezca una conexión SSH (o Telnet) con el iDRAC6 mediante las credenciales correctas.

Se mostrará la petición SMCLP (/admin1->).

Destinos de SM-CLP

Tabla 12-2 contiene una lista de los destinos que se proporcionan por medio de SM-CLP para sustentar las operaciones que se describen en la Tabla 12-1 anteriormente.

Tabla 12-2. Destinos de SM-CLP

Destino	Definiciones
admin1	Dominio de admin
admin1/profiles1	Perfiles registrados en el iDRAC6
admin1/hdwr1	Hardware
admin1/system1	Destino de sistema administrado
admin1/system1/redundancyset1	Suministro de energía
admin1/system1/redundancyset1/pwrsupply*	Suministro de energía del sistema administrado
admin1/system1/sensors1	Sensores del sistema administrado
admin1/system1/capabilities1	Capacidades de recopilación del sistema administrado SMASH
admin1/system1/capabilities1/ pwrcap1	Capacidades de utilización de la alimentación del sistema administrado
admin1/system1/capabilities1/ elecap1	Capacidades de destino del sistema administrado
admin1/system1/logs1	Destino de las recolecciones de registro.
admin1/system1/logs1/log1	Entrada de registro de eventos del sistema (SEL)
admin1/system1/logs1/log1/ record*	Una entrada individual del registro de eventos del sistema en el sistema administrado
admin1/system1/settings1	Configuración de recopilación del sistema administrado SMASH
admin1/system1/settings1/ pwrmaxsetting1	Configuración de asignación de alimentación máxima del sistema administrado
admin1/system1/settings1/ pwrminsetting1	Configuración de asignación de alimentación mínima del sistema administrado
admin1/system1/capacities1	Capacidades de recopilación del sistema administrado SMASH
admin1/system1/consoles1	Recopilación SMASH de las consolas del sistema administrado
admin1/system1/usbredirectsap1	SAP de redirección de USB de medios virtuales
admin1/system1/usbredirectsap1/remotesap1	SAP de redirección de USB de destino de medios virtuales
admin1/system1/sp1	Procesador de servicio
admin1/system1/sp1/timesvc1	Servicio de hora del procesador de servicio
admin1/system1/sp1/capabilities1	Recopilación SMASH de las capacidades del procesador de servicio
admin1/system1/sp1/capabilities1/clpcap1	Capacidades del servicio CLP
admin1/system1/sp1/capabilities1/pwrmgtcap1	Capacidades del servicio de administración del estado de la alimentación en el sistema
admin1/system1/sp1/capabilities1/ipcap1	Capacidades de la interfaz IP
admin1/system1/sp1/capabilities1/dhcpcap1	Capacidades del cliente DHCP
admin1/system1/sp1/capabilities1/NetPortCfgcap1	Capacidades de configuración del puerto de red
admin1/system1/sp1/capabilities1/usbredirectcap1	SAP de redirección de USB de capacidades de medios virtuales
admin1/system1/sp1/capabilities1/vmsapcap1	Capacidades SAP de medios virtuales
admin1/system1/sp1/capabilities1/swinstallsvccap1	Capacidades de servicio de instalación de software
admin1/system1/sp1/capabilities1/acctmgtcap*	Capacidades del servicio de administración de cuenta
admin1/system1/sp1/capabilities1/adcap1	Capacidades de Active Directory
admin1/system1/sp1/capabilities1/rolemgtcap*	Capacidades de administración basada en funciones locales
admin1/system1/sp1/capabilities/PwrutilmgtCap1	Capacidades de administración de utilización de la alimentación
admin1/system1/sp1/capabilities/metriccap1	Capacidades del servicio métrico
admin1/system1/sp1/capabilities1/elecap1	Capacidades de autenticación multifactor
admin1/system1/sp1/capabilities1/lanendptcap1	Capacidades del punto final de (puerto Ethernet) LAN
admin1/system1/sp1/logs1	Recopilación de registros del procesador de servicio
admin1/system1/sp1/logs1/log1	Registro de sistema
admin1/system1/sp1/logs1/log1/record*	Entrada del registro de sistema
admin1/system1/sp1/settings1	Recopilación de configuración del procesador de servicio
admin1/system1/sp1/settings1/ clpsetting1	Datos de configuración del servicio CLP
admin1/system1/sp1/settings1/ ipsettings1	Datos de configuración de la asignación de la interfaz IP (estática)
admin1/system1/sp1/settings1/ ipsettings1/staticipsettings1	Datos de configuración de la asignación de la interfaz IP estática
admin1/system1/sp1/settings1/ ipsettings1/dnssettings1	Datos de configuración de cliente DNS
admin1/system1/sp1/settings1/ ipsettings2	Datos de configuración de la asignación de la interfaz IP (DHCP)
admin1/system1/sp1/settings1/ ipsettings2/dhcpsettings1	Datos de configuración del cliente DHCP
admin1/system1/sp1/clpsvc1	Servicio de protocolo del servicio CLP

admin1/system1/sp1/clpsvc1/ clpendpt*	Punto final del protocolo del servicio CLP
admin1/system1/sp1/clpsvc1/ tcpendpt*	Punto final TCP del protocolo del servicio CLP
admin1/system1/sp1/jobq1	Cola de trabajo del protocolo del servicio CLP
admin1/system1/sp1/jobq1/job*	Trabajo del protocolo del servicio CLP
admin1/system1/sp1/pwrmgtsvc1	Servicio de administración del estado de la alimentación
admin1/system1/sp1/ipcfgsvc1	Servicio de configuración de la interfaz IP
admin1/system1/sp1/ipendpt1	Punto final del protocolo de la interfaz IP
admin1/system1/sp1/ ipendpt1/gateway1	Puerta de enlace de la interfaz IP
admin1/system1/sp1/ ipendpt1/dhcpendpt1	Punto final del protocolo del cliente DHCP
admin1/system1/sp1/ ipendpt1/dnsendpt1	Punto final del protocolo del cliente DNS
admin1/system1/sp1/ipendpt1/ dnsendpt1/dnsserver*	Servidor del cliente DNS
admin1/system1/sp1/NetPortCfgsvc1	Servicio de configuración del puerto de red
admin1/system1/sp1/lanendpt1	Punto final del LAN
admin1/system1/sp1/ lanendpt1/enetport1	Puerto Ethernet
admin1/system1/sp1/VMediaSvc1	Servicio de medios virtuales
admin1/system1/sp1/ VMediaSvc1/tcpendpt1	Punto final del protocolo TCP de medios virtuales
admin1/system1/sp1/swid1	Identidad de software
admin1/system1/sp1/ swinstallsvc1	Servicio de instalación de software
admin1/system1/sp1/ account1-16	Cuenta de autenticación multifactor (MFA)
admin1/sysetm1/sp1/ account1-16/identity1	Cuenta de identidad de usuario local
admin1/sysetm1/sp1/ account1-16/identity2	Cuenta de identidad de IPMI (LAN)
admin1/sysetm1/sp1/ account1-16/identity3	Cuenta de identidad de IPMI (Serie)
admin1/sysetm1/sp1/ account1-16/identity4	Cuenta de identidad CLP
admin1/system1/sp1/acctsvc1	Servicio de administración de cuenta de MFA
admin1/system1/sp1/acctsvc2	Servicio de administración de cuenta de IPMI
admin1/system1/sp1/acctsvc3	Servicio de administración de cuenta de CLP
admin1/system1/sp1/group1-5	Grupo de Active Directory
admin1/system1/sp1/ group1-5/identity1	Identidad de Active Directory
admin1/system1/sp1/ADSvc1	Servicio de Active Directory
admin1/system1/sp1/rolesvc1	Servicio de autorización basada en funciones (RBA) local
admin1/system1/sp1/rolesvc1/ Role1-16	Función local
admin1/system1/sp1/rolesvc1/ Role1-16/privilege1	Privilegio de la función local
admin1/system1/sp1/rolesvc1/ Role17-21/	Función de Active Directory
admin1/system1/sp1/rolesvc1/ Role17-21/privilege1	Privilegio de Active Directory
admin1/system1/sp1/rolesvc2	Servicio de RBA de IPMI
admin1/system1/sp1/rolesvc2/ Role1-3	Función de IPMI
admin1/system1/sp1/rolesvc2/ Role4	Función de la comunicación en serie en la LAN (SOL) de IPMI
admin1/system1/sp1/rolesvc3	Servicio CLP de RBA
admin1/system1/sp1/rolesvc3/ Role1-3	Función de CLP
admin1/system1/sp1/rolesvc3/ Role1-3/privilege1	Privilegio de la función de CLP
admin1/system1/sp1/ pwrutilmgtsvc1	Servicio de administración de la utilización de la alimentación
admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1	Datos de la configuración de la asignación de alimentación actual de servicio de administración de la utilización de la alimentación
admin1/system1/sp1/metricsvc1	Servicio métrico
/admin1/system1/sp1/metricsvc1/cumbmd1	Definición métrica de base acumulativa

/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	Valor métrico de base acumulativa
/admin1/system1/sp1/metricsvc1/cumwattamd1	Definición métrica de concentración acumulativa de vatios
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	Valor métrico de concentración acumulativa de vatios
/admin1/system1/sp1/metricsvc1/cumampamd1	Definición métrica de concentración acumulativa de amp
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	Valor métrico de concentración acumulativa de amp
/admin1/system1/sp1/metricsvc1/loamd1	Definición métrica de concentración baja
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	Valor métrico de concentración baja
/admin1/system1/sp1/metricsvc1/hiamd1	Definición métrica de concentración alta
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	Valor métrico de concentración alta
/admin1/system1/sp1/metricsvc1/avgamd1	Definición métrica de concentración promedio
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	Valor métrico de concentración promedio

---

Regresar a la página de contenido

Regresar a la página de contenido

Instalación del sistema operativo mediante VMCLI

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

La utilidad de interfaz de línea de comandos de medios virtuales (VMCLI) es una interfaz de línea de comandos que ofrece las funciones de medios virtuales de la estación de administración al iDRAC6 en el sistema remoto. Por medio de la VMCLI y los métodos con secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad VMCLI en su red corporativa.

Antes de comenzar

Antes de usar la utilidad VMCLI, asegúrese de que los sistemas remotos de destino y la red de la empresa cumplan con los requisitos que se mencionan en las siguientes secciones.

Requisitos de los sistemas remotos

El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Una área compartida de red debe tener los componentes siguientes:

- Los archivos de sistema operativo
- Los controladores necesarios
- Los archivos de imagen de inicio del sistema operativo

El archivo de imagen debe ser un CD de sistema operativo o una imagen ISO de CD/DVD, con un formato de inicio estándar en la industria.

Creación de un archivo de imagen iniciable

Antes de instalar el archivo de imagen en los sistemas remotos, compruebe que el sistema compatible puede iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz web de usuario del iDRAC6 y luego reinicie el sistema.

Las siguientes secciones contienen información específica para la creación de archivos de imagen para los sistemas Linux y Microsoft® Windows®.

Creación de un archivo de imagen para los sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen iniciable para el sistema Linux.

Para ejecutar la utilidad, abra una petición de comandos y escriba lo siguiente:

```
dd if=<dispositivo_de_entrada> of=<archivo_de_salida>
```

Por ejemplo:

```
dd if=/dev/sdc0 of=mycd.img
```

Creación de un archivo de imagen para los sistemas Windows

Al elegir una utilidad replicadora de datos para los archivos de imagen de Windows, seleccione una utilidad que copie el archivo de imagen y los sectores de inicio de CD/DVD.

Preparación para la instalación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que la estación de administración pueda acceder.
2. Copie los archivos de sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen iniciable preconfigurado para instalación, cree el archivo. Incluya los programas o secuencias de comandos que se vayan a utilizar para los procedimientos de instalación del sistema operativo.

   Por ejemplo, para instalar un sistema operativo Windows, el archivo de imagen puede incluir programas que sean similares a los métodos de instalación que utiliza Systems Management Server (SMS) de Microsoft.

   Al momento de crear el archivo de imagen, haga lo siguiente:

   - Siga los procedimientos estándares de instalación basada en red
   - Marque la imagen de instalación como *de sólo lectura* para garantizar que cada sistema de destino se inicie y se ejecute en el mismo procedimiento de instalación
4. Realice uno de los procedimientos siguientes:
   - Integre **IPMItool** y VMCLI en la aplicación existente de instalación del sistema operativo. Use la secuencia de comandos de ejemplo **vm6deploy** como guía para usar la utilidad.
   - Utilice la secuencia de comandos **vm6deploy** existente para instalar el sistema operativo.

Instalación del sistema operativo

Use la utilidad VMCLI y la secuencia de comandos **vm6deploy** que se incluye con la utilidad para instalar el sistema operativo en los sistemas remotos.

Antes de comenzar, revise la secuencia de comandos **vm6deploy** de ejemplo que se incluye con la utilidad VMCLI. La secuencia de comandos muestra los pasos detallados que se necesitan para instalar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para instalar el sistema operativo en los sistemas remotos de destino.

1. Haga una lista de las direcciones IPv4 del iDRAC6 de los sistemas remotos que serán instalados en el archivo de texto **ip.txt**, una dirección IPv4 por línea.
2. Inserte un CD o DVD iniciable de sistema operativo en la unidad correspondiente del cliente.
3. Ejecute **vm6deploy** en la línea de comandos.

Para ejecutar la secuencia de comandos **vm6deploy**, introduzca el siguiente comando en el indicador de comandos:

```
vm6deploy -r ip.txt -u <usuario_del_idrac> -p <contraseña_del_idrac> -c {<imagen_iso9660> | <ruta_de_acceso>} -f
{<imagen_de_disquete>|<ruta_de_acceso>}
```

donde:

- <*usuario_del_idrac*> es el nombre de usuario del iDRAC6, por ejemplo, **root**
- <*contraseña_del_idrac*> es la contraseña del usuario del iDRAC6, por ejemplo, **calvin**
- <*imagen_iso9660*> es la ruta de acceso de la imagen ISO9660 del CD o DVD de instalación del sistema operativo
- <*ruta_de_acceso*> es la ruta de acceso del dispositivo que contiene el CD, DVD o disquete de instalación del sistema operativo
- <*imagen_de_disquete*> es la ruta de acceso a una imagen de disquete válida

La secuencia de comandos **vm6deploy** pasa las opciones de línea de comandos a la utilidad **VMCLI**. Consulte "Opciones de la línea de comandos" para obtener detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta a la opción **vmcli -r**. Si el argumento de la opción **-r** es el nombre de un archivo existente, la secuencia de comandos leerá las direcciones IPv4 del iDRAC6 del archivo especificado y ejecutará la utilidad **VMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, deberá ser la dirección de un solo iDRAC6. En este caso, la opción **-r** funciona como se describe en la utilidad **VMCLI**.

Uso de la utilidad VMCLI

La utilidad VMCLI es una interfaz de línea de comandos que admite secuencias de comandos y que suministra las funciones de medios virtuales de la estación de administración al iDRAC6.

La utilidad VMCLI presenta las siguientes características:

NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.

- Dispositivos de medios extraíbles o archivos de imagen que son congruentes con los complementos de medios virtuales
- Finalización automática cuando la opción del firmware del iDRAC6 para iniciar una vez está activada
- Comunicaciones seguras con el iDRAC6 por medio de la capa de sockets seguros (SSL)

Antes de ejecutar la utilidad, asegúrese de que cuenta con privilegios de usuario de medios virtuales en el iDRAC6.

Si el sistema operativo admite los privilegios de administrador o una pertenencia a grupos o privilegio específico del sistema operativo, también deberá tener privilegios de administrador para poder ejecutar el comando VMCLI.

El administrador del sistema cliente controla los privilegios y grupos de usuarios, por consiguiente, controla cuáles usuarios pueden ejecutar la utilidad.

Para sistemas Windows, se deben tener privilegios de usuario avanzado para poder ejecutar la utilidad VMCLI.

En los sistemas Linux, se puede acceder a la utilidad VMCLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando brinda un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos del usuario. Para agregar o editar usuarios en el grupo VMCLI, el administrador usa el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de VMCLI (o a la secuencia de comandos de VMCLI) a fin de obtener acceso al iDRAC6 en el sistema remoto y ejecutar la utilidad.

Instalación de la utilidad VMCLI

La utilidad VMCLI se encuentra en el DVD *Dell Systems Management Tools and Documentation*, que se incluye en el paquete de software Dell OpenManage System Management. Para instalar la utilidad, inserte el DVD *Dell Systems Management Tools and Documentation* en la unidad DVD del sistema y siga las instrucciones que aparecen en la pantalla.

El DVD *Dell Systems Management Tools and Documentation* contiene los productos de software de administración de sistemas más recientes, incluso los diagnósticos, la administración de almacenamiento, el servicio de acceso remoto y la utilidad IPMItool. Este DVD también contiene archivos léame con la información más reciente sobre los productos de software de administración de sistemas.

Además, el DVD *Dell Systems Management Tools and Documentation* incluye **vm6deploy**, una secuencia de comandos de ejemplo que ilustra el uso de las utilidades VMCLI e IPMItool para instalar software en varios sistemas remotos.

NOTA: La secuencia de comandos **vm6deploy** depende de otros archivos que están presentes en el directorio de la misma cuando se instala. Si desea usar la secuencia de comandos desde otro directorio, deberá copiar todos los archivos con ella. Si la utilidad IPMItool no está instalada, es necesario copiarla junto con los otros archivos.

Opciones de la línea de comandos

La interfaz VMCLI es idéntica en los sistemas Windows y Linux.

El formato del comando VMCLI es el siguiente:

`VMCLI` *`[parámetro] [opciones_de_shell_de_sistema_operativo]`*

En la sintaxis de la línea de comandos se distingue entre mayúsculas y minúsculas. Consulte "Parámetros de VMCLI" para obtener más información.

Si el sistema remoto acepta los comandos y el iDRAC6 autoriza la conexión, el comando seguirá ejecutándose hasta que se presente cualquiera de los siguientes casos:

- La conexión de VMCLI termina por algún motivo.
- El proceso se termina manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, se puede usar el Administrador de tareas para terminar el proceso.

Parámetros de VMCLI

Dirección IP del iDRAC6

`-r` *`<dirección_IP_del_iDRAC>[:<puerto_SSL_del_iDRAC>]`*

Este parámetro proporciona la dirección IPv4 del iDRAC6 y el puerto SSL, con los que la utilidad debe establecer una conexión de medios virtuales con el iDRAC6 de destino. Si introduce un nombre de DDNS o una dirección IPv4 que no son válidos, aparecerá un mensaje de error y el comando terminará.

<*dirección_IP_del_iDRAC*> es una dirección IPv4 válida y única, o bien, el nombre de sistema dinámico de nombres de dominio (DDNS) del iDRAC6 (si se admite). Si el <*puerto_SSL_de_iDRAC*> se omite, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado del iDRAC6.

Nombre de usuario del iDRAC6

`-u` *`<nombre_de_usuario_del_iDRAC>`*

Este parámetro proporciona el nombre de usuario del iDRAC6 que ejecutará los medios virtuales.

El <*nombre_de_usuario_del_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales del iDRAC6

Si la autenticación del iDRAC6 falla, aparecerá un mensaje de error y el comando terminará.

Contraseña de usuario del iDRAC6

`-p` *<contraseña_de_usuario_del_iDRAC>*

Este parámetro proporciona la contraseña para el usuario del iDRAC6 especificado.

Si la autenticación del iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco / disquete

`-f {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido (para sistemas Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

NOTA: Para la utilidad VMCLI, no se admiten puntos de montaje.

Este parámetro especifica el dispositivo o archivo que va a proporcionar el medio virtual de disco o disquete.

Por ejemplo, un archivo de imagen se especifica como:

`-f c:\temp\myfloppy.img` (sistema Windows)

`-f /tmp/myfloppy.img` (sistema Linux)

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Configure el sistema operativo para proteger contra escritura una imagen de disquete que no desea que se sobrescriba.

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`--f /dev/sdb4 # 4th partition on device /dev/sdb` (sistema Linux)

NOTA: Red Hat® Enterprise Linux® versión 4 no admite ni admitirá varios LUN. Sin embargo, el kernel admite esta funcionalidad, pero debe habilitar Red Hat Enterprise Linux versión 4 para que reconozca un dispositivo SCSI con varios LUN; para ello, siga estos pasos.

1. Edite **/etc/modprobe.conf** y agregue la siguiente línea:
   options scsi_mod max_luns=8
   (Puede especificar 8 LUN o cualquier otro número mayor que 1).

2. Obtenga el nombre de la imagen del kernel; para ello, escriba el siguiente comando en la línea de comandos:

   `uname -r`

3. Vaya al directorio **/boot** y elimine el archivo de imagen del kernel, cuyo nombre determinó en el Paso 2:

   `mkinitrd /boot/initrd-'uname -r'.img `uname -r'`

4. Reiniciar el servidor.

5. Ejecute el siguiente comando para confirmar que se admiten varios LUN para la cantidad de LUN que especificó en el Paso 1:

   `cat /sys/modules/scsi_mod/max_luns`

Si el dispositivo tiene capacidad de protección contra escritura, utilice esta capacidad para garantizar que los medios virtuales no escribirán en el medio.

Omita este parámetro de la línea de comandos si no va a virtualizar disquetes. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD / DVD

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas

Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o archivo que proporcionará el medio virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

`-c c:\temp\mydvd.img` (sistemas Windows)

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Microsoft® Windows®)

`-c /dev/cdrom` (sistemas Linux)

Omita este parámetro de la línea de comandos si no va a virtualizar discos CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disquete o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

`-v`

Este parámetro se usa para mostrar la versión de la utilidad VMCLI. Si no se proporcionan otras opciones además de interruptores, el comando terminará sin mensajes de error.

Mostrar la ayuda

`-h`

Este parámetro muestra un resumen de los parámetros de la utilidad VMCLI. Si no se proporcionan otras opciones además de conmutadores, el comando terminará sin errores.

Datos cifrados

`-e`

Cuando se incluya este parámetro en la línea de comandos, VMCLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el iDRAC6 en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifrará.

NOTA: El uso de esta opción no cambia el estado de cifrado de los medios virtuales que se muestra a *activado* en otras interfaces de configuración del iDRAC6 como RACADM o la interfaz web.

Opciones de shell de sistema operativo de VMCLI

Las siguientes funciones del sistema operativo se pueden usar en la línea de comandos de VMCLI:

- stderr/stdout redirection: desvía los mensajes de salida impresos hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad VMCLI.

  NOTA: La utilidad VMCLI no lee la entrada estándar (**stdin**). En consecuencia, la redirección de **stdin** no es necesaria.

- Ejecución en segundo plano: de manera predeterminada, la utilidad VMCLI se ejecuta en primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en el segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

La última técnica es útil en programas de secuencias de comandos, ya que permite que la secuencia de comandos proceda después de que se inicia un nuevo proceso para el comando VMCLI (de lo contrario, la secuencia de comandos se bloqueará hasta que el programa VMCLI finalice). Cuando se inician varias instancias de VMCLI de esta manera, y una o varias de las instancias de comando se finalizan manualmente, utilice las instalaciones específicas del sistema operativo para listar y finalizar procesos.

Códigos de retorno de VMCLI

Cuando se presentan errores, se envían mensajes de texto en inglés a la salida estándar de errores.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la interfaz de administración de plataforma inteligente (IPMI)

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Configuración de IPMI

Esta sección proporciona información sobre cómo configurar y usar la interfaz IPMI del iDRAC6 La interfaz incluye lo siguiente:

- IPMI mediante la LAN
- IPMI en la conexión serie
- Comunicación en serie en la LAN

El iDRAC6 es totalmente compatible con IPMI 2.0. Puede configurar la IPMI del iDRAC6 por medio de:

- La interfaz gráfica del usuario del iDRAC6 de su explorador
- Una utilidad de código abierto, como *IPMItool*
- El shell de IPMI de Dell™ OpenManage™, *ipmish*
- RACADM

Para obtener más información sobre cómo usar el shell de IPMI, ipmish, consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* que se encuentra disponible en **support.dell.com\manuals**.

Para obtener más información sobre cómo usar RACADM, consulte "Uso de RACADM de manera remota".

Configuración de IPMI por medio de la interfaz web

Para obtener más información, consulte "Configuración de IPMI".

Configuración de IPMI por medio de la interfaz de línea de comandos de RACADM

1. Inicie sesión en el sistema remoto por medio de cualquiera de las interfaces de RACADM. Consulte "Uso de RACADM de manera remota".
2. Configure la IPMI en la LAN.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

   NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

   a. Actualice los privilegios de canal de IPMI.

      En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>
      ```

      donde <*nivel*> es uno de los siguientes:

      - 2 (Usuario)
      - 3 (Operador)
      - 4 (Administrador)

      Por ejemplo, para definir el privilegio de canal de LAN de IPMI en 2 (usuario), escriba el comando siguiente:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

NOTA: La IPMI de iDRAC6 es compatible con el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>`

donde <*clave*> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1`

a. Actualice el nivel de privilegios mínimo de SOL de IPMI.

NOTA: El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación IPMI 2.0.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>`

donde <*nivel*> es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para configurar los privilegios de IPMI como 2 (usuario), escriba el siguiente comando:

`racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2`

b. Actualice la velocidad en baudios de la SOL de IPMI.

NOTA: Para redirigir la consola serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_en_baudios>`

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo:

`racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600`

c. Active la SOL para un usuario individual.

NOTA: Es posible activar o desactivar la SOL para cada usuario individual.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <identificación> 2`

donde *<identificación>* es la identificación única del usuario.

4. Configure la conexión serie de IPMI.

a. Cambie el modo de conexión serie de IPMI al valor adecuado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgSerial -o cfgSerialConsoleEnable 0`

b. Establezca la velocidad en baudios de la conexión serie de IPMI.

Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <velocidad_en_baudios>`

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo:

`racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600`

c. Active el control de flujo del hardware de la conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

d. Establezca el nivel mínimo de privilegios de canal de conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>
```

donde *<nivel>* es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para definir los privilegios de canal de conexión serie de IPMI en 2 (usuario), escriba el siguiente comando:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. Compruebe que el multiplexor serie esté configurado correctamente en el programa de configuración del BIOS.

- Reinicie el sistema.
- Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
- Haga clic en **Comunicación en serie**.
- En el menú **Conexión serie**, compruebe que **Conector serie externo** esté definido como **Dispositivo de acceso remoto**.
- Guarde los cambios y salga del programa de configuración del BIOS.
- Reinicie el sistema.

La configuración de IPMI ha terminado.

Si la conexión serie de IPMI está en modo de terminal, usted puede configurar los siguientes valores adicionales por medio de los comandos **racadm config cfgIpmiSerial**:

- Control de eliminación
- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Uso de la interfaz serie de acceso remoto de IPMI

Los siguientes modos están disponibles en la interfaz serie de IPMI:

- **Modo de terminal de IPMI**: admite comandos ASCII provenientes de una terminal serie. El conjunto de comandos tiene un número limitado de comandos (que incluye el control de alimentación) y admite comandos de IPMI sin procesar que se introducen como caracteres ASCII hexadecimales.
- **Modo básico de IPMI**: admite una interfaz binaria para acceso a programa, como el shell de IPMI (IPMISH) que se incluye con la utilidad de administración de la placa base (BMU).

Para configurar el modo de IPMI por medio de RACADM:

1. Desactive la interfaz serie del RAC.

   En la petición de comandos, escriba:

   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```

2. Active el modo IPMI adecuado.

   Por ejemplo, en la petición de comandos, escriba:

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 ó 1>
   ```

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6" para obtener información.

Configuración de la comunicación en serie en la LAN mediante la interfaz web

Para obtener más información, consulte "Configuración de IPMI".

NOTA: Puede usar la comunicación en serie en la LAN con las siguientes herramientas de Dell OpenManage: SOLProxy e IPMItool. Para obtener más información, consulte la *Guía del usuario de utilidades del controlador de administración de la placa base de Dell OpenManage* en **support.dell.com\manuals**.

Regresar a la página de contenido

Regresar a la página de contenido

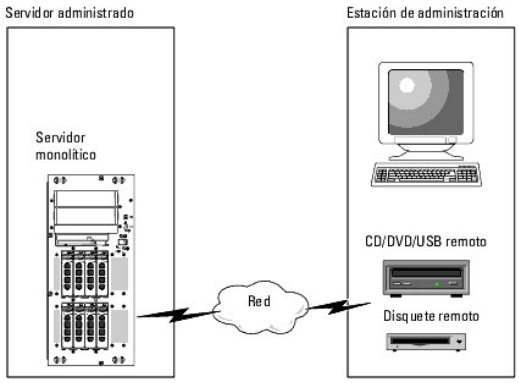
Configuración y uso de medios virtuales

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Información general

El componente **Medios virtuales**, que puede encontrar a través del visor de redirección de consola, permite que el servidor administrado tenga acceso a medios conectados a un sistema remoto en la red. La Figura 15-1 muestra la arquitectura general de los **medios virtuales**.

Figura 15-1. Arquitectura general de medios virtuales



Por medio de los **medios virtuales**, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar controladores o incluso instalar nuevos sistemas operativos de manera remota desde las unidades CD/DVD y disquete virtuales.

NOTA: Los **medios virtuales** requieren una amplitud de banda de red mínima disponible de 128 Kbps.

Los **medios virtuales** definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: un dispositivo de disquete y un dispositivo de disco óptico.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando los **medios virtuales** se conectan de forma manual o automática, todas las solicitudes de acceso a la unidad virtual de CD o disquete provenientes del servidor administrado son dirigidas a la estación de administración por la red. Conectar los **medios virtuales** es equivalente a insertar un medio en un dispositivo físico del sistema administrado. Cuando los **medios virtuales** están en estado de conexión, los dispositivos virtuales en el sistema administrado aparecen como dos unidades sin los medios instalados.

La Tabla 15-1 lista las conexiones compatibles de unidades ópticas virtuales y de disquete virtuales.

NOTA: Si cambia los **medios virtuales** mientras están conectados podría detener la secuencia de inicio del sistema.

Tabla 15-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disquete virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disquete heredada de 1,44 con disquete de 1,44	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disquete USB con un disquete de 1,44	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disquete de 1,44	Unidad USB de CD-ROM con disco CD-ROM
Disco extraíble USB	

Estación de administración con Windows

Para ejecutar el componente de **medios virtuales** en una estación de administración que ejecuta el sistema operativo Microsoft® Windows®, instale una versión compatible de Internet Explorer o Firefox con Java Runtime Environment (JRE). Consulte "Exploradores web admitidos" para obtener detalles.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Firefox. Consulte "Exploradores web admitidos" para obtener más información.

Se requiere Java Runtime Environment (JRE) para ejecutar el complemento de redirección de consola. Puede descargar JRE desde el sitio **java.sun.com**. Se recomienda la versión 1.6 o superiores de JRE.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Sistema**→ **Consola / Medios**.
3. Haga clic en **Configuración**→ **Medios virtuales** para configurar los valores de los medios virtuales.

   La Tabla 15-2 describe los valores de configuración de los **medios virtuales**.
4. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 15-3.

Tabla 15-2. Propiedades de configuración de los medios virtuales

Atributo	Valor
Estado conectado de los medios remotos	**Conectar**: conecta inmediatamente los **medios virtuales** al servidor. **Desconectar**: desconecta inmediatamente los **medios virtuales** del servidor. **Conectar automáticamente**: conecta los **medios virtuales** al servidor únicamente cuando se inicia una sesión de medios virtuales.
Máx. de sesiones	Muestra el número máximo de sesiones de **medios virtuales** permitidas, que es siempre 1.
Sesiones activas	Muestra el número actual de sesiones de medios virtuales.
Cifrado activado para medios virtuales	Seleccione o deseleccione la casilla de verificación para activar o desactivar el cifrado en conexiones de **medios virtuales**. Si está seleccionada, activa el cifrado; si no está seleccionada, desactiva el cifrado.
Emulación de disquete	Indica si los **medios virtuales** aparecen como unidad de disquete o como memoria USB en el servidor. Si se selecciona **Emulación de disquete**, el dispositivo **medios virtuales** aparecerá como dispositivo de disquete en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB.
Activar el inicio una vez	Marque esta casilla para activar la opción **Iniciar una vez**. Utilice este atributo para que el inicio se realice desde los medios virtuales la próxima vez. El sistema se iniciará desde la siguiente entrada en el orden de inicio. Esta opción cierra automáticamente la sesión de **medios virtuales** después de que el sistema se inicia una vez.

Tabla 15-3. Botones de la página de configuración

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración**.
Aplicar cambios	Guarda todos los nuevos valores de configuración de la página **Configuración**.

Ejecución de los medios virtuales

PRECAUCIÓN: No emita un comando racreset cuando esté ejecutando una sesión de medios virtuales. Si lo hace, se pueden producir resultados no deseables, incluso la pérdida de datos.

NOTA: La aplicación de la ventana del visor de consola debe permanecer activa mientras usted accede a los medios virtuales.

NOTA: Realice los pasos siguientes para permitir que Red Hat® Enterprise Linux® (versión 4) reconozca un dispositivo SCSI con múltiples unidades lógicas (LUN):

1. Agregue la línea siguiente a **/ect/modprobe**:

   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp

2. Reinicie el servidor.

3. Ejecute los siguientes comandos para ver el CD/DVD virtual o el disquete virtual:

   cat /proc/scsi/scsi

NOTA: A través de los medios virtuales, puede virtualizar una unidad de disquete/memoria USB/imagen/memoria y una unidad óptica de su estación de administración para que esté disponible como unidad (virtual) en el servidor administrado.

Configuraciones compatibles de medios virtuales

Puede activar los medios virtuales para una unidad de disquete y una unidad de discos ópticos. Sólo se puede virtualizar una unidad a la vez por cada tipo de medio.

Las unidades de disquete que se admiten incluyen una imagen de disquete o una unidad de disquete disponible. Las unidades ópticas que se admiten incluyen un máximo de una unidad óptica disponible o un archivo de imagen ISO.

Conexión de los medios virtuales

Realice los pasos siguientes para ejecutar medios virtuales:

1. Abra un explorador de web compatible en la estación de administración. Para obtener más información, consulte "Exploradores web admitidos".

2. Inicie la interfaz web del iDRAC6. Para obtener más información, consulte "Acceso a la interfaz web".

3. Seleccione **Systema→ Consola / Medios**.

   Aparecerá la página **Redirección de consola y medios virtuales**. Si desea cambiar los valores de cualquiera de los atributos mostrados, consulte "Configuración de los medios virtuales".

   NOTA: Es posible que aparezca **Archivo de imagen de disquete** bajo **Unidad de disquete** (si se aplica), pues este dispositivo se puede virtualizar como un disquete virtual. Puede seleccionar una unidad óptica y una unidad de disquete/memoria USB al mismo tiempo para virtualizar.

   NOTA: Las letras de unidad de los dispositivos virtuales en el servidor administrado no coinciden con las letras de unidades físicas en la estación de administración.

   NOTA: Es posible que los **medios virtuales** no funcionen correctamente en los clientes con sistema operativo Windows que estén configurados con seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador del sistema.

4. Haga clic en **Iniciar el visor**.

   NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo preguntará qué desea hacer con el archivo. Elija la opción de **Abrir con el programa** y después seleccione la aplicación **javaws**, que se encuentra en el subdirectorio **bin** del directorio de instalación de JRE.

   La aplicación **Agente KVM del iDRAC** se ejecuta en otra ventana.

5. Haga clic en **Herramientas→ Ejecutar Medios virtuales**.

   Aparecerá el asistente de redirección de medios.

   NOTA: No cierre este asistente a menos que desee terminar la sesión de medios virtuales.

6. Si hay algún medio conectado, deberá desconectarlo antes de conectar otro medio. Deseleccione la casilla a la izquierda del medio que desea desconectar.

7. Marque la casilla que aparece junto a los tipos de medios que desea conectar.

   Si desea conectar una imagen de disquete o una imagen ISO, introduzca la ruta de acceso (en el equipo local) a la imagen o haga clic en el botón **Agregar imagen...** y busque la imagen**.**

   Los medios están conectados y la ventana de **estado** se actualiza.

Desconexión de los medios virtuales

1. Haga clic en **Herramientas→ Ejecutar Medios virtuales**.

2. Deseleccione la casilla que está junto a los medios que desea desconectar.

   Los medios se desconectarán y se actualizará la ventana de **estado**.

3. Haga clic en **Salir** para cerrar el asistente de redirección de medios.

Inicio desde los medios virtuales

El BIOS del sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disquete virtuales. Durante la POST (Power-On Self-Test [autoprueba de encendido]), ingrese a la ventana de configuración del BIOS y verifique que las unidades virtuales estén activadas y que aparezcan en el orden correcto.

Para cambiar el valor en el BIOS, realice los pasos a continuación:

1. Inicie el servidor administrado.
2. Presione <F2> para ingresar a la ventana de configuración del BIOS.
3. Desplácese a la secuencia de inicio y presione <*Entrar*>.

   En la ventana emergente, aparece una lista de las unidades ópticas y de disquete virtuales con los dispositivos estándar de inicio.
4. Asegúrese de que la unidad virtual esté activada y que aparezca como el primer dispositivo con medio iniciable. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.
5. Guarde los cambios y salga.

   El servidor administrado se reinicia.

   El servidor administrado intenta iniciarse a partir de un dispositivo iniciable con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio iniciable está presente, el sistema se iniciará a partir del dispositivo virtual. De lo contrario, el sistema ignorará el dispositivo; como ocurriría con un dispositivo físico que no tiene medios iniciables.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas en terminar. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de **medios virtuales** puede tardar menos de 15 minutos en terminar. Consulte "Instalación del sistema operativo" para obtener más información.

1. Verifique lo siguiente:
   - El CD de instalación de sistema operativo está insertado en la unidad de CD de la estación de administración.
   - La unidad de CD local está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección "Inicio desde los medios virtuales" para asegurarse de que el BIOS está configurado para que inicie desde la unidad de CD a partir de la que se realiza la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

Es importante seguir estos pasos para la instalación de varios discos:

1. Desasigne el CD/DVD virtualizado (redirigido) desde la consola de medios virtuales.
2. Inserte el siguiente CD/DVD en la unidad óptica remota.
3. Asigne (redirija) este CD/DVD desde la consola de medios virtuales.

   Es posible que si inserta un nuevo CD/DVD en la unidad óptica remota sin realizar la reasignación no funcione.

Función Iniciar una vez

La función Iniciar una vez le ayuda a cambiar el orden del inicio temporalmente para iniciar desde un dispositivo remoto de medios virtuales. Esta función se usa junto con medios virtuales, generalmente, mientras se instalan sistemas operativos.

NOTA: Para usar esta función, debe tener el privilegio **Configurar el iDRAC6**.

NOTA: Los dispositivos remotos deben redirigirse mediante el uso de medios virtuales para usar esta función.

Uso de la función Iniciar una vez:

1. Encienda el servidor e ingrese al administrador de inicio del BIOS.

2. Cambie la secuencia de inicio para iniciar desde el dispositivo de medios virtuales remoto.

3. Conéctese al iDRAC6 por medio de la interfaz web y haga clic en **Sistema**→ **Consola / Medios**→ **Configuración**.

4. Marque la opción **Activar el inicio una vez** en Medios virtuales.

5. Realice un ciclo de encendido en el servidor.

   El servidor se inicia desde el dispositivo de medios virtuales remoto. La próxima vez que el servidor se reinicia, la conexión remota de medios virtuales está desconectada.

   NOTA: Los medios virtuales deben estar en estado **Conectado** para que las unidades virtuales aparezcan en la secuencia de inicio. Verifique que los medios iniciables estén presentes en la unidad virtualizada para activar la opción **Iniciar una vez**.

Utilización de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En sistemas con Windows, las unidades de medios virtuales se montan automáticamente cuando están conectadas y se configuran con una letra de unidad.

La utilización de las unidades virtuales desde el interior de Windows es similar a la utilización de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estarán disponibles en el sistema cuando se haga clic en la unidad y se examine el contenido de la misma.

Sistemas con Linux

En función de la configuración del software del sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, monte manualmente las unidades con el comando **mount** de Linux.

Preguntas frecuentes sobre medios virtuales

La Tabla 15-4 contiene las preguntas y respuestas frecuentes.

Tabla 15-4. Uso de los medios virtuales: preguntas frecuentes

Pregunta	Respuesta
Algunas veces noto que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?	Cuando expira el tiempo de la red, el firmware del iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Si los valores de configuración de los medios virtuales se cambian en la interfaz web del iDRAC6 o con los comandos de RACADM local, se desconectarán todos los medios conectados al momento de aplicar el cambio de configuración. Para restablecer la conexión con la unidad virtual, use el asistente de medios virtuales.
¿Qué sistemas operativos son compatibles con el iDRAC6?	Consulte "Sistemas operativos admitidos" para ver una lista de los sistemas operativos admitidos.
¿Qué exploradores web admiten el iDRAC6?	Consulte "Exploradores web admitidos" para ver una lista de los exploradores web admitidos.
¿Por qué a veces se pierde mi conexión de cliente?	• Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD en la unidad de CD del sistema cliente, en nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede expirar el tiempo y se puede perder la conexión cuando el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior. • Cuando expira el tiempo de la red, el firmware del iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Asimismo, alguien puede haber cambiado los valores de configuración de los medios virtuales en la interfaz web o mediante comandos de RADACM. Para restablecer la conexión con el disco virtual, use la función de **Medios virtuales**.
La instalación del sistema operativo Windows mediante medios virtuales parece tardar demasiado. ¿Por qué?	Si instala el sistema operativo Windows por medio del DVD *Dell Systems Management Tools and Documentation* y la conexión de red es lenta, es posible que el procedimiento de instalación requiera más tiempo para acceder a la interfaz web del iDRAC6 debido a la latencia de la red. Mientras la ventana de instalación no indique el progreso de la instalación, significa que el procedimiento de instalación está en progreso.
¿Cómo configuro mi dispositivo virtual como dispositivo iniciable?	En el servidor administrado, acceda a la configuración del BIOS y haga clic en el menú de inicio. Localice el CD virtual, el disco flexible virtual o la memoria flash virtual y cambie el orden de dispositivo de inicio según corresponda. Para configurar el dispositivo virtual como dispositivo iniciable, presione la tecla de barra espaciadora en la secuencia de inicio de la configuración de CMOS. Por ejemplo, para iniciar a partir de una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.
¿A partir de qué tipos de medios puedo iniciar el sistema?	El iDRAC6 le permite iniciar desde los siguientes medios de inicio: • Medios de CDROM/DVD de datos • Imagen ISO 9660 • Imagen de disquete o disquete de 1,44

	• Una memoria USB a la que el sistema operativo reconoce como disco extraíble • Una imagen de memoria USB
¿Cómo puedo hacer que mi memoria USB sea iniciable?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para hacer que la memoria USB de Dell funcione como dispositivo de inicio. Usted puede iniciar también con un disco de arranque de Windows 98 y copiar los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, desde una ventana del símbolo del sistema DOS, escriba el comando siguiente: `sys a: x: /s` donde *x*: es la memoria USB que desea hacer iniciable.
No puedo encontrar mi dispositivo de disquete virtual/CD virtual en un sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE® Linux. Mis medios virtuales están conectados y estoy conectado al disquete remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disquete virtual y la unidad de CD virtual de manera similar. Para montar la unidad de disquete virtual, encuentre el nodo de dispositivo que Linux asigna a la unidad de disquete virtual. Realice los pasos siguientes para encontrar y montar correctamente la unidad de disquete virtual: 1. Abra una ventana del símbolo del sistema de Linux y ejecute el siguiente comando: grep "Virtual Floppy" /var/log/messages 2. Localice la última entrada de dicho mensaje y anote la hora. 3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: grep "hh:mm:ss" /var/log/messages donde: *hh:mm:ss* es la hora del mensaje que el comando grep informó en el paso 1. 4. En el paso 3, lea el resultado del comando grep y localice el nombre del dispositivo que se asigna al disco virtual Dell. 5. Asegúrese de que está conectado a la unidad de disquete virtual. 6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
No puedo encontrar mi dispositivo de disquete virtual/CD virtual en un sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux. Mis medios virtuales están conectados y estoy conectado al disquete remoto. ¿Qué debo hacer?	*(Continuación de la respuesta)* Para montar la unidad de CD virtual, encuentre el nodo de dispositivo que Linux asigna a la unidad de CD virtual. Realice los siguientes pasos para buscar y montar la unidad de CD virtual: 1. Abra una ventana del símbolo del sistema de Linux y ejecute el siguiente comando: grep "CD virtual" /var/log/messages 2. Localice la última entrada de dicho mensaje y anote la hora. 3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: grep "hh:mm:ss" /var/log/messages donde hh:mm:ss es la hora del mensaje que el comando grep informó en el paso 1. 4. En el paso 3, lea el resultado del comando grep y localice el nombre de dispositivo que se asignó a "CD virtual de Dell". 5. Asegúrese de que está conectado a la unidad de CD virtual. 6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/CD donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
Cuando ejecuté una actualización de firmware de manera remota por medio de la interfaz web del iDRAC6, mis unidades virtuales en el servidor se desmontaron. ¿Por qué?	Las actualizaciones de firmware hacen que el iDRAC6 se restablezca, que abandone la conexión remota y que desmonte las unidades virtuales.
¿Por qué todos mis dispositivos USB se desconectan después de que conecto un dispositivo USB?	Los dispositivos de medios virtuales y los dispositivos flash virtuales están conectados como dispositivo USB compuesto al BUS USB del host y comparten un puerto USB común. Cuando un medio virtual o dispositivo USB flash virtual se conecta o se desconecta del BUS USB del host, todos los medios virtuales y los dispositivos flash virtual se desconectan momentáneamente del BUS USB del host y luego se conectan nuevamente. Si el sistema operativo del host está usando un dispositivo de medios virtuales, debe evitar conectar o desconectar uno o más dispositivos de medios virtuales o flash virtual. Se recomienda que conecte todos los dispositivos USB necesarios primero, antes de usarlos.
¿Qué hace el botón restablecer USB?	Restablece los dispositivos USB remotos y locales conectados al servidor.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de una tarjeta multimedia vFlash para utilizar con el iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

La tarjeta multimedia vFlash es una tarjeta Secure Digital (SD) que se conecta en la ranura para tarjeta opcional del iDRAC6 Enterprise ubicada en la parte posterior del sistema. Proporciona espacio de almacenamiento y actúa como un dispositivo USB flash común. Para obtener información sobre cómo instalar y desinstalar del sistema la tarjeta multimedia vFlash, consulte el *Manual del propietario de hardware* en **support.dell.com\manuals**.

Configuración de la tarjeta multimedia vFlash por medio de la interfaz web del iDRAC6

Activación y desactivación de la tarjeta multimedia vFlash

NOTA: La opción **Flash virtual activado** sólo está habilitada si hay una tarjeta multimedia vFlash. Si no insertó una tarjeta, aparecerá el siguiente mensaje:

```
SD Card not inserted. Please insert an SD card of size greater than 256MB. (Tarjeta SD no insertada. Inserte una tarjeta SD de tamaño mayor a 256MB.)
```

1. Asegúrese de que la tarjeta vFlash esté instalada.
2. Abra el explorador web compatible e inicie sesión en la interfaz web del iDRAC6.
3. Seleccione **Sistema** en el árbol del sistema.
4. Haga clic en la lengüeta **Flash virtual**.

   Aparecerá la pantalla **Flash virtual**.
5. Seleccione la opción **Flash virtual activado** para habilitar la tarjeta multimedia vFlash. Al activar la opción, el archivo de imagen **ManagedStore.IMG** creado en la tarjeta SD quedará expuesto como una memoria USB del tamaño seleccionado. La opción de flash virtual sólo puede activarse si en la tarjeta SD hay una imagen **ManagedStore.IMG** válida. Para desactivarla, deje en blanco la opción.

   NOTA: Los archivos ManagedStore.IMG y ManagedStore.ID vistos en la página de la interfaz gráfica del usuario de *Flash virtual* no estarán visibles en el sistema operativo del servidor de host sino en la tarjeta SD.
6. Haga clic en **Aplicar cambios**.

Formato de la tarjeta multimedia vFlash

NOTA: La opción **Formato** sólo está habilitada si hay una tarjeta multimedia vFlash. Además, la tarjeta sólo puede formatearse si la opción Flash virtual está deshabilitada.

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Sistema** en el árbol del sistema.
3. Haga clic en la lengüeta **Flash virtual**.

   Aparecerá la pantalla **Flash virtual**.
4. Deje en blanco la opción **Flash virtual activa**.
5. Haga clic en **Formato** para crear el archivo de imagen flash virtual **ManagedStore.IMG** en la tarjeta SD. En la tarjeta SD también se crea el archivo de texto **ManagedStore.ID**, que brinda información sobre la imagen flash virtual.

   Aparecerá una casilla de alerta con la advertencia de que todas las imágenes que estén en la tarjeta se borrarán durante el proceso, y solicitará confirmación. Haga clic en **Aceptar** para continuar.

   Aparecerá una barra de estado que muestra el progreso del proceso de formateo.

Cargar una imagen de disco

1. Asegúrese de que el tamaño del archivo de imagen no supere los 256 MB.

   NOTA: Si bien su tarjeta vFlash puede ser de tamaño mayor que 256 MB, sólo se puede acceder a 256 MB en este momento.

   NOTA: El uso de flash virtual permite almacenar imágenes de inicio de emergencia y herramientas de diagnóstico directamente en la tarjeta multimedia vFlash. El archivo de imagen puede ser una imagen de disquete iniciable de DOS como archivo ***.img** para Windows o un archivo **diskboot.img** de los medios de Red Hat® Enterprise Linux® para Linux. El archivo **diskboot.img** puede usarse para crear un disco de rescate o un disco para ejecutar instalaciones de red. Flash virtual puede utilizarse para alojar una imagen persistente para uso general o de emergencia en el futuro.

2. Inicie sesión en la interfaz web del iDRAC6.

3. Seleccione **Sistema** en el árbol del sistema.

4. Haga clic en la lengüeta **Flash virtual**.

   Aparecerá la pantalla **Flash virtual**.

5. Deje en blanco la opción **Flash virtual activa**.

6. En la sección **Unidad flash virtual**, introduzca la ruta de acceso al archivo de imagen o haga clic en **Examinar** para ubicarlo en el sistema.

   Haga clic en **Cargar**.

   Aparecerá una barra de estado que muestra el progreso del proceso de carga.

NOTA: Puede cargar una imagen ISO iniciable en la partición flash virtual, aunque ya no será iniciable. Para que la imagen IMG sea iniciable, convierta la imagen ISO a una imagen IMG.

Visualización del tamaño de la memoria flash virtual

El menú desplegable **Tamaño de la memoria flash virtual** muestra la configuración de tamaño actual.

Configuración de la tarjeta multimedia vFlash con RACADM

Activación y desactivación de la tarjeta multimedia vFlash

Abra una consola local al servidor, inicie sesión e introduzca:

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ó 0 ]
```

en donde `1` significa activada y `0` significa desactivada.

NOTA: Para obtener más información acerca de **cfgRacVirtual**, incluidos los detalles de mensajes de salida, consulte "cfgRacVirtual".

NOTA: El comando RACADM sólo funcionará si hay una tarjeta multimedia vFlash. Si no hay una tarjeta, aparecerá el siguiente mensaje: *ERROR: Unable to perform the requested operation. Ensure that a non−write protected SD Card is inserted*. (*ERROR: no es posible realizar la operación solicitada. Verifique si se insertó una tarjeta SD protegida contra escritura*.)

Restablecimiento de la tarjeta multimedia vFlash

Abra una consola de texto de Telnet/SSH en el servidor, inicie sesión e introduzca:

```
racadm vmkey reset
```

PRECAUCIÓN: Cuando la tarjeta multimedia vFlash se restablece con el comando RACADM, se restablece el tamaño de la memoria en 256 MB y se borran todos los datos existentes.

NOTA: Para obtener más información acerca del comando vmkey, consulte "vmkey". El comando RACADM sólo funcionará si hay una tarjeta multimedia vFlash. Si no hay una tarjeta, aparecerá el siguiente mensaje: *ERROR: Unable to perform the requested operation. Ensure that a SD Card is inserted*. (*ERROR: no es posible realizar la operación solicitada. Verifique si se insertó una tarjeta SD*.)

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de energía

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Los sistemas Dell™ PowerEdge™ traen muchas características nuevas y mejoradas de administración de energía. El diseño de toda la plataforma, desde el hardware al firmware hasta el software de administración de sistemas, está orientado a la eficacia energética, y a la supervisión y administración de energía.

El diseño base del hardware ha sido optimizado desde una perspectiva de alimentación:

- Alta eficiencia de suministro de energía y reguladores de voltaje han sido incorporados en el diseño.
- Donde es posible, los componentes con alimentación más baja son seleccionados.
- El diseño de chasis ha optimizado el flujo de aire a través del sistema para minimizar la alimentación del ventilador.

Los sistemas PowerEdge brindan muchas características para controlar y manejar la alimentación:

- **Presupuesto e inventario de alimentación:** durante el inicio, un inventario del sistema permite calcular el presupuesto de alimentación de la configuración actual.
- **Límite de alimentación:** los sistemas pueden ser regulados para mantener un límite de alimentación especificado.
- **Supervisión de alimentación:** el iDRAC6 consulta a los suministros de alimentación para reunir las medidas de alimentación. El iDRAC6 junta un historial de las medidas de alimentación y calcula los promedios y picos actuales. Con la interfaz web del iDRAC6 se puede ver esta información en la pantalla **Supervisión de alimentación**.

Inventario, presupuesto y límite de alimentación

Desde una perspectiva de utilización, usted podría tener una cantidad limitada de enfriamiento en el nivel estante. Con un límite de alimentación definido por el usuario, usted puede permitir alimentación como sea necesaria para los requisitos de su desempeño.

El iDRAC6 supervisa el consumo de energía y dinámicamente regula los procesadores para que cumplan con su nivel límite definido, que maximiza el desempeño y a su vez cumple con los requisitos de alimentación.

Supervisión de alimentación

El iDRAC6 supervisa el consumo de energía en los servidores PowerEdge en forma continua. El iDRAC6 calcula los siguientes valores de alimentación y proporciona la información a través de su interfaz web o de línea de comandos de RACADM:

- Consumo acumulativo de energía
- Alimentación promedio, mínima y máxima
- Valores de capacidad adicional de alimentación
- Consumo de energía (también puede verlo en gráficas en la interfaz web)

Configuración y administración de energía

Se puede usar la interfaz web del iDRAC6 y la interfaz de línea de comandos (CLI) RACADM para administrar y configurar los controles de alimentación en el sistema PowerEdge. Expresamente, usted puede:

- Ver el estado de alimentación del servidor.
- Ejecutar operaciones de control de alimentación en el servidor (por ejemplo, encendido, apagado, reinicio del sistema, ciclo de alimentación).
- Ver la información del presupuesto de alimentación para el servidor y las unidades de alimentación instaladas, como consumo de energía potencial mínimo y máximo.
- Ver y configurar el umbral del presupuesto de alimentación del servidor.

Ver el estado de las unidades de suministro de energía

La página de **Suministros de energía** muestra el estado y la clasificación de las unidades del suministro de energía instaladas en el servidor.

Acceso a la interfaz web

Para ver el estado de las unidades de suministro de energía:

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Suministros de energía** en el árbol del sistema. La página de **Suministros de energía** muestra y proporciona la siguiente información:
   - **Estado de redundancia de suministros de energía**: los valores posibles son:
     - **Completas**: Los suministros de energía PS1 y PS2 son de la misma clase y funcionan apropiadamente.
     - **Perdidas**: Los suministros de energía PS1 y PS2 son diferentes clases y un de ellos no funciona correctamente. No existe redundancia.
     - **Desactivada**: Solo uno de los suministros de energía está disponible. No existe redundancia.
   - **Elementos de suministro de energía individuales:** los posibles valores son:
   - **Estado** muestra lo siguiente:
     - **Correcto** indica que la unidad de suministro de energía está presente y se comunica con el servidor.
     - **Advertencia** indica que sólo se emitieron alertas de advertencia y el administrador debe tomar una medida correctiva. Si no se realizan acciones correctivas, se pueden producir fallas de alimentación críticas o graves que pueden afectar la integridad del servidor.
     - **Grave** indica que se ha emitido al menos un alerta de falla. El estado de falla indica una falla de alimentación en el servidor y se debe realizar una acción correctiva inmediatamente.
   - **Ubicación** muestra el nombre de la unidad de suministro de energía: PS-n donde n es el número de suministro de energía.
   - **Tipo** muestra el tipo de suministro de energía, como CA o CC (conversión de voltaje de CA a CC o de CC a CA).
   - **Potencia de entrada** muestra la potencia de entrada de suministro de energía, que es una carga máxima de corriente alterna que el sistema podría colocar en el centro de datos.
   - **Potencia máxima** muestra la potencia máxima de suministro de energía, que es la corriente continua disponible para el sistema. Este valor se utiliza para confirmar que la capacidad de suministro de energía suficiente está disponible para la configuración del sistema.
   - **Estado en línea** indica el estado de la alimentación de los suministros de energía: presente y correcto, entrada perdida, ausente o falla predictiva.
   - **Versión de FW** muestra la versión de firmware del suministro de energía.

NOTA: La potencia máxima es diferente de la potencia de entrada debido a la eficiencia del suministro de energía. Por ejemplo, si la eficiencia del suministro de energía es 89% y la potencia máxima es 717 W, la potencia de entrada se estima en 797 W.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

Ver el presupuesto de alimentación

El servidor proporciona descripciones generales del estado de la alimentación del subsistema de energía en la página **Información del presupuesto de alimentación**.

Por medio de la interfaz web

NOTA: Para realizar acciones de administración de energía, se debe contar con privilegios de **Administrador**.

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en la lengüeta **Administración de energía**.
3. Seleccione la opción **Presupuesto de alimentación**.
4. Se muestra la página **Estado del presupuesto de alimentación**.

La primera tabla muestra los límites mínimos y máximos de los umbrales de alimentación especificados por el usuario para la configuración del sistema actual. Estos representan el rango de consumos de corriente alterna que usted podría configurar como límite del sistema. Una vez seleccionado, este límite podría ser la carga de corriente alterna máxima que el sistema pudiera colocar en el centro de datos.

Consumo de energía potencial mínimo muestra el valor más bajo del umbral de presupuesto de alimentación que usted podría especificar.

Consumo de energía potencial máximo muestra el valor más alto del umbral de presupuesto de alimentación que usted podría especificar. Este valor es también el consumo de alimentación máximo absoluto de la configuración actual del sistema.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

NOTA: Para obtener más información acerca de cfgServerPower, incluso los detalles de mensajes de salida, consulte "cfgServerPower".

Umbral de presupuesto de alimentación

El umbral de presupuesto de alimentación, si está activado, permite establecer un límite de energía para el sistema. El rendimiento del sistema se ajusta en forma dinámica a fin de mantener el consumo de energía cerca del umbral determinado. El consumo de energía real puede ser menor en cargas de trabajo más livianas y puede exceder el umbral momentáneamente hasta completar los ajustes de rendimiento.

Si marca **Activado** para Umbral de presupuesto de alimentación, el sistema implementará el umbral especificado por el usuario. Si **no marca** el valor Umbral de presupuesto de alimentación, el sistema no tendrá límite de alimentación. Por ejemplo, para una determinada configuración del sistema, el consumo de energía potencial máximo es 700 W y el consumo de energía potencial mínimo es 500 W. Puede especificar y activar un umbral de presupuesto de alimentación para reducir el consumo desde los 650 W actuales hasta 525 W. Desde ese punto, el desempeño del sistema se ajustará dinámicamente para mantener el consumo de energía de modo que no exceda el umbral especificado del usuario de 525 W.

Acceso a la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en la lengüeta **Administración de energía**.
3. Seleccione la opción **Presupuesto de alimentación**. Se muestra la página **Estado del presupuesto de alimentación**.
4. Introduzca un valor en vatios, BTU/h o porcentaje en la tabla **Umbral de presupuesto de alimentación**. El valor que especifique en vatios o BTU/h será el valor límite del umbral del presupuesto de alimentación. Si especifica un valor de porcentaje, será un porcentaje de intervalo de consumo de energía potencial máximo a mínimo. Por ejemplo, un umbral de 100% significa un consumo de energía potencial máximo, mientras que 0% significa un consumo de energía potencial mínimo.

   NOTA: El umbral de presupuesto de alimentación no puede ser mayor al consumo de energía potencial máximo ni menor al consumo de energía potencial mínimo.

5. Marque **Activado** para activar el umbral o no lo marque. Si especifica **Activado**, el sistema implementará el umbral especificado por el usuario. Si no lo **marca**, el sistema no tendrá límite de alimentación.
6. Haga clic en **Aplicar cambios**.

Uso de RACADM

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <valor límite de alimentación en vatios>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <valor límite de alimentación en BTU/h>

racadm config -g cfgServerPower -o - cfgServerPowerCapPercent <valor límite de alimentación en porcentaje>
```

NOTA: Cuando configure el umbral de presupuesto de alimentación en BTU/h, la conversión a vatios se redondea al número entero más cercano. Cuando se vuelve a leer el umbral de presupuesto de alimentación, la conversión de vatios a BTU/h vuelve a redondearse del mismo modo. Como resultado, el valor escrito podría ser nominalmente diferente al valor leído; por ejemplo, un umbral establecido en 600 BTU/h será leído como 601 BTU/h.

Ver la supervisión de alimentación

Por medio de la interfaz web

Para ver la información de supervisión de alimentación:

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Supervisión de alimentación** en el árbol del sistema. Se muestra la página **Supervisión de alimentación**.

La información brindada en la página **Supervisión de alimentación** se describe a continuación.

Supervisión de alimentación

- **Estado**: **Correcto** indica que las unidades de de suministro de energía están presentes y se comunican con el servidor; **Advertencia** indica que una alerta de advertencia ha sido emitida; y **Grave** indica que una alerta de falla ha sido emitida.
- **Nombre de la sonda**: nivel del sistema de la placa base. La descripción indica que la sonda está supervisada por su ubicación en el sistema.
- **Lectura**: el consumo de energía actual en vatios o BTU/h.

Amperaje

- **Ubicación**: muestra el nombre de la unidad de suministro de energía: PS-n donde n es el número de suministro de energía.
- **Lectura**: el consumo de energía actual en amperios.

Estadísticas de seguimiento de alimentación

NOTA: Hay un defecto por resolver en la lista de hora actual y hora de máximo. El valor mostrado debajo de la hora actual es en realidad la hora de máximo, y el valor debajo de la hora de máximo es la hora actual.

- **Acumulado** Indica el consumo acumulado actual de energía del servidor medido desde la entrada de los suministros de energía. Los valores son visualizados en KWh y el valor acumulado, que es el total de energía utilizada por el sistema. Puede restablecer el valor con el botón **Restablecer acumulado**.
- **Amperios máximos** especifica el valor máximo actual dentro el intervalo especificado por las horas de inicio y actual. Puede restablecer el valor con el botón **Restablecer máximos**.
- **Vatios máximos** especifica el valor máximo de alimentación dentro el intervalo especificado por las horas de inicio y actual. Puede restablecer el valor con el botón **Restablecer máximos**.
- **Hora de inicio** muestra la fecha y la hora registrados cuando se borró por última vez el valor de consumo de energía del sistema y comenzó el nuevo ciclo de mediciones. Para **Acumulado**, puede restablecer este valor con el botón **Restablecer acumulado**, pero persistirá luego de una operación de restablecimiento o falla del sistema. Para **Amperios máximos** y **Vatios máximos**, puede restablecer este valor con el botón **Restablecer máximos**, pero también persistirá luego de una operación de restablecimiento o falla del sistema.
- **Hora de fin** para **Acumulado** muestra la fecha y hora actuales en las que se calculó el consumo de energía del sistema para su visualización. Para **Amperios máximos** y **Vatios máximos**, los campos **Hora de fin** muestran la hora cuando estos picos ocurrieron.

NOTA: Se mantienen estadísticas de seguimiento de alimentación luego de todos los restablecimientos del sistema para reflejar toda la actividad en el intervalo entre la hora de inicio y de fin. El botón **Restablecer máximos** restablecerá el campo respectivo en cero. En la tabla siguiente, la información de consumo de energía no se mantiene luego de restablecimientos del sistema, por lo que se restablecerá a cero en dichas ocasiones. Los valores de alimentación que se muestran son promedios acumulados en el intervalo de tiempo respectivo (minuto, hora, día y semana previos). Debido a que los intervalos de tiempo de inicio y fin pueden ser distintos de aquellos de las estadísticas de seguimiento de alimentación, los valores máximos de alimentación (máximos en vatios en comparación con consumo máximo de energía) pueden ser distintos.

Consumo de energía

- Muestra el consumo de energía promedio, máximo y mínimo en el sistema para el último minuto, hora, día y semana.
- Consumo de energía promedio: promedio sobre minuto, hora, día y mes anteriores.
- Consumo de energía máximo y mínimo: los consumos de energía máximo y mínimo observados dentro del intervalo de tiempo determinado.
- Hora de máximo y mínimo: la hora en el que se producen consumos de energía máximos y mínimos.

Capacidad adicional

La capacidad adicional instantánea del sistema muestra la diferencia entre la alimentación disponible en las unidades de suministro de energía y el consumo de energía actual del sistema.

La capacidad adicional máxima del sistema muestra la diferencia entre la alimentación disponible en las unidades de suministro de energía y el consumo de energía máximo del sistema.

Mostrar gráfica

Al hacer clic en esta tecla, se muestra la gráfica de la alimentación del iDRAC6 y el consumo actual en vatios y amperios, respectivamente, en la última hora. El usuario tiene la opción de ver estas estadísticas hasta una semana antes, con el menú desplegable provisto arriba de las gráficas.

NOTA: Cada uno de los puntos de información de la gráfica representa el promedio de lecturas en un lapso de 5 minutos. Como resultado, es posible que la gráfica no refleje fluctuaciones breves de alimentación ni tampoco el consumo actual.

Ejecución de operaciones de control de alimentación en el servidor

NOTA: Para realizar acciones de administración de energía, debe contar con privilegios de **Administrador de control de chasis**.

El iDRAC6 le permite efectuar en forma remota varias acciones de administración de energía, como un apagado ordenado.

Por medio de la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en la lengüeta **Administración de energía**. Se muestra la página **Control de alimentación**.
3. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
   - **Encender el sistema** enciende el sistema (equivalente a pulsar el botón de encendido cuando el servidor está apagado). Esta opción se desactivará si el servidor ya está encendido.
   - **Apagar el sistema** apaga la alimentación del servidor. Esta opción se desactivará si el sistema ya está apagado.
   - **NMI (interrupción no enmascarable)** genera una NMI para interrumpir la operación del sistema.
   - **Apagado normal** apaga el sistema.
   - **Restablecer el sistema** (reinicio mediante sistema operativo) reinicia el sistema sin apagarlo. Esta acción se desactivará si el sistema ya está apagado.
   - **Ciclo de encendido del sistema** (inicio en frío) apaga el sistema y luego lo reinicia. Esta opción se desactivará si el sistema ya está apagado.
4. Haga clic en **Aplicar**. Aparecerá un cuadro de diálogo para solicitar una confirmación.
5. Haga clic en **Aceptar** para realizar la acción de administración de energía (por ejemplo, hacer que se restablezca el sistema).

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el servidor, inicie sesión y escriba:

```
racadm serveraction <acción>
```

donde `<acción>` es powerup, powerdown, powercycle, hardreset o powerstatus.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la utilidad de configuración del iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Información general

La utilidad de configuración del iDRAC es un entorno de configuración previo al inicio que permite visualizar y establecer parámetros para el iDRAC6 y para el servidor administrado. Expresamente, usted puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware de plano posterior primario
- Activar o desactivar la red de área local del iDRAC
- Activar o desactivar la IPMI sobre LAN
- Configurar los parámetros de LAN
- Configurar los medios virtuales
- Configurar la tarjeta inteligente
- Cambiar el nombre de usuario administrativo y la contraseña
- Restablecer la configuración predeterminada de fábrica del iDRAC
- Ver o borrar los mensajes del registro de eventos del sistema (SEL)
- Configurar LCD
- Configurar servicios del sistema

Las tareas que puede realizar utilizando la utilidad de configuración del iDRAC también se pueden realizar con el uso de otras utilidades proporcionadas por iDRAC o el software Dell™ OpenManage™, incluida la interfaz web, la interfaz de línea de comandos SM-CLP y la interfaz de línea de comandos de RACADM local.

Inicio de la utilidad de configuración del iDRAC

1. Encienda o reinicie el servidor con el botón de encendido que se encuentra en el frente del servidor.
2. Cuando aparezca el mensaje **Presione <Ctrl-E> para la configuración de acceso remoto dentro de los 5 segundos...** presione inmediatamente <Ctrl><E>.

NOTA: Si el sistema operativo comienza a cargarse antes de que usted presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el servidor e inténtelo otra vez.

Aparecerá la utilidad de configuración del iDRAC. Las dos primeras dos líneas ofrecen información sobre el firmware del iDRAC6 y las revisiones del firmware de plano posterior primario. Los niveles de revisión pueden ser útiles para determinar si una actualización de firmware es necesaria.

El firmware del iDRAC6 es una parte de la información relacionada con las interfaces externas, como la interfaz web, SM-CLP y las interfaces web. El firmware de plano posterior primario es la parte del firmware que se conecta con el entorno de hardware del servidor y lo supervisa.

Uso de la utilidad de configuración del iDRAC

Bajo los mensajes de revisión del firmware, el resto de la utilidad de configuración del iDRAC es un menú de opciones a las que puede tener acceso por medio de las teclas <Flecha hacia arriba> y <Flecha hacia abajo>.

- Si una opción del menú conduce a un submenú o a un campo de texto editable, presione <Entrar> para acceder a la opción y <Esc> para salir de la misma después de terminar de configurarla.
- Si un elemento tiene valores que se pueden seleccionar, como Sí/No o Activado/Desactivado, presione <Flecha izquierda>, <Flecha derecha> o <Barra espaciadora> para elegir un valor.
- Si un elemento no se puede editar, aparecerá en azul. Algunos elementos se pueden editar en función de otras selecciones que usted haga.
- La línea en la parte inferior de la pantalla muestra instrucciones relacionadas con el elemento actual. Puede presionar <F1> para mostrar la ayuda del elemento actual.
- Cuando haya terminado de usar la utilidad de configuración del iDRAC, presione <Esc> para ver el menú de salida, donde podrá elegir si desea guardar o descartar los cambios o volver a la utilidad.

Las secciones siguientes describen las opciones del menú de la utilidad de configuración del iDRAC.

LAN del iDRAC6

Use la <Flecha izquierda>, <Flecha derecha> y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**.

La LAN del iDRAC6 está activada en la configuración predeterminada. La LAN debe estar activada para permitir el uso de los servicios del iDRAC6 tales como la interfaz web, Telnet/SSH, la redirección de consola y los medios virtuales.

Si elige desactivar la LAN, aparecerá la siguiente advertencia:

```
iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF.

Press any key to clear the message and continue.

(La interfaz del iDRAC6 fuera de banda se desactivará si el canal de LAN está desactivado.

Presione cualquier tecla para quitar el mensaje y continuar.)
```

El mensaje le informa que, además de los servicios a los que tiene acceso a través de la conexión directa del iDRAC mediante HTTP, HTTPS, Telnet o los puertos SSH, el tráfico de red de administración fuera de banda, por ejemplo, los mensajes de IPMI que se envían al iDRAC6 desde una estación de administración, no se recibe cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN del iDRAC6.

IPMI en la LAN

Presione la <Flecha izquierda>, <Flecha derecha> y la barra espaciadora para elegir entre **Activada** y **Desactivada**. Cuando se seleccione **Desactivada**, el iDRAC6 no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivada**, aparecerá la siguiente advertencia:

```
iDRAC IPMI Over LAN Out-of-Band interface will be disabled if the LAN Channel is OFF. (La interfaz del iDRAC IPMI fuera de banda se desactivará si el canal de LAN está desactivado.
```

Presione cualquier tecla para quitar el mensaje y continuar. Consulte "LAN del iDRAC6" para ver una explicación del mensaje.

Parámetros de LAN

Presione <Entrar> para mostrar el submenú de parámetros de la LAN. Cuando haya terminado de configurar los parámetros de la LAN, presione <Esc> para volver al menú anterior.

Tabla 18-1. Parámetros de LAN

Elemento	Descripción
Valores comunes	
Selección de NIC	Presione la <Flecha derecha>, <Flecha izquierda > y la barra espaciadora para cambiar entre los modos. Los modos disponibles son **Dedicado, Compartido**, **Compartido con LOM2 de protección contra fallas** y **Compartido con todos los LOM2 de protección contra fallas**. Estos modos le permitirán al iDRAC6 utilizar la interfaz correspondiente para la comunicación con el mundo externo.
Dirección MAC	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC6.
Activar VLAN	Seleccione **Activado** para permitir el filtrado de LAN virtual para el iDRAC6.
Identificación de VLAN	Si **Activar VLAN** está configurado como **Activado**, introduzca cualquier valor de identificación de VLAN entre 1 y 4094.
VLAN	Si **Activar VLAN** está configurado como **Activado**, seleccione la prioridad de VLAN entre 0 y 7.
Registrar el nombre del iDRAC6	Seleccione **Activado** para registrar el nombre del iDRAC6 en el servicio DNS. Seleccione **Desactivado** si no desea que los usuarios puedan encontrar el nombre del iDRAC6 en el DNS.
Nombre del iDRAC6	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Entrar> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Presione <Entrar> cuando haya terminado de modificar el nombre del iDRAC6. Presione <Esc> para volver al menú anterior. El nombre del iDRAC6 debe ser un nombre de host DNS válido.
Nombre de dominio de DHCP	Seleccione **Activado** si desea obtener el nombre de dominio de un servicio DHCP de la red. Seleccione **Desactivado** si desea especificar el nombre de dominio.
Nombre de dominio	Si **Nombre de dominio de DHCP** esta **Desactivado**, presione <Entrar> para modificar el campo de texto **Nombre de dominio actual**. Presione <Entrar> cuando haya terminado de modificarlo. Oprima <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.
Cadena de nombre del host	Presione <Entrar> para editarla. Introduzca el nombre del host para alertas de excepción de eventos de plataforma (PET).
Alerta de LAN activada	Seleccione **Activado** para permitir un alerta de PET de LAN.
Entrada de política de alerta 1	Seleccione **Activar** o **Desactivar** para activar el primer destino de alerta.
Destino de alerta 1	Si **Alerta de LAN activada** está **Activada**, introduzca la dirección del IP donde se enviarán las alertas de PET de LAN.
Configuración de IPv4	Habilite o deshabilite la compatibilidad para conexión IPv4.
IPv4	Seleccione **Activado** o **Desactivado** para la compatibilidad con el protocolo IPv4.

Clave de cifrado RMCP+	Presione <Entrar> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado RMCP+ es una cadena hexadecimal de 40 caracteres (caracteres 0-9, a-f y A-F). RMCP+ es una extensión de IPMI que agrega la autenticación y el cifrado a IPMI. El valor predeterminado es una cadena de 40 ceros.
Origen de dirección IP	Seleccione entre **DHCP** y **Estática**. Cuando se selecciona DHCP, los campos **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se obtienen de un servidor DHCP. Si no se encuentra ningún servidor DHCP en la red, los campos tomarán valores de ceros. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar**.**
Dirección IP de Ethernet	Si la opción **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6 La dirección predeterminada es **192.168.0.120.**
Máscara de subred	Si **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección de máscara de subred que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la máscara de subred para el iDRAC6. El valor predeterminado es **255.255.255.0**.
Puerta de enlace predeterminada	Si **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada. El valor predeterminado es **192.168.0.1**.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores DNS a continuación.
Servidor DNS 1	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Servidor DNS 2	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del segundo servidor DNS.
Configuración de IPv6	Active o desactive la compatibilidad para la conexión IPv6.
Origen de dirección IP	Seleccione entre **AutoConfig** y **Estática**. Cuando se selecciona **AutoConfig**, los campos **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se obtienen de DHCP. Cuando se selecciona **Estática**, las opciones **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se pueden editar.
Dirección IPv6 1	Si **Origen de dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6
Longitud del prefijo	Configura la longitud del prefijo de la dirección IPv6. Se puede valuar entre 1 y 128, inclusive.
Puerta de enlace predeterminada	Si **Origen de dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada.
Dirección IPv6 local	Ésta es la **dirección IPv6 local** no editable de la interfaz de red del iDRAC.
Dirección IPv6 2	Ésta es la **dirección IPv6 2** no editable de la interfaz de red del iDRAC.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores DNS a continuación.
Servidor DNS 1	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Servidor DNS 2	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Configuraciones de LAN avanzadas	
Negociación automática	Si la **Selección de NIC** se configura a **Dedicada**, seleccione entre **Activada** y **Desactivada.** Cuando se selecciona **Activada**, la **configuración de velocidad de LAN** y la **configuración dúplex de LAN** se configuran automáticamente.
Configuración de la velocidad de LAN	Si **Negociación automática** se establece en **Desactivado**, seleccione entre 10 Mbps y 100 Mbps.
Configuración dúplex de LAN	Si **Negociación automática** se establece en **Desactivado**, seleccione entre **Semi dúplex y Dúplex total.**

Configuración de medios virtuales

Medios virtuales

Presione <Entrar>y seleccione **Desconectado, Conectado** o **Autoconectado.** Cuando se selecciona **Conectado**, los dispositivos de medios virtuales se conectan al bus USB y están listos para su uso durante las sesiones de **Redirección de consola**.

Si selecciona **Desconectado**, los usuarios no podrán acceder a los dispositivos de medios virtuales durante las sesiones de **redirección de consola**.

NOTA: Para usar una unidad flash USB con la función de **Medios virtuales**, la opción **Tipo de emulación de unidad flash USB** debe estar establecida como **Disco duro** en la utilidad de configuración del BIOS. Se puede acceder a la utilidad de configuración del BIOS al presionar <F2> durante el arranque del servidor. Si el **Tipo de emulación de la unidad flash USB** se establece como **Automático**, la unidad flash aparecerá como unidad de disquete en el sistema.

Unidad flash virtual

Presione <Entrar> para seleccionar **Desactivado** o **Activado.**

Desactivado/Activado hace que todos los dispositivos virtuales del bus USB se **desconecten** y **conecten**.

Desactivado hace que la memoria virtual flash se elimine y deje de estar disponible para su uso.

NOTA: Este campo puede ser de sólo lectura si una tarjeta SD con un tamaño superior a 256 MB no está presente en la ranura Express card del iDRAC6.

Inicio de sesión con tarjeta inteligente

Presione <Entrar> para seleccionar **Activado** o **Desactivado**. Esta opción configura la característica de inicio de sesión con tarjeta inteligente. Las opciones disponibles son **Activado**, **Desactivado** y **Activado con RACADM.**

NOTA: Cuando seleccione **Activado**, **IPMI sobre LAN** será desactivado y bloqueado para edición.

Configuración de servicios del sistema

Servicios del sistema

Presione <Entrar> para seleccionar **Activado** o **Desactivado**. Para obtener más información, consulte la *Guía del usuario de Dell Unified Server Configurator* disponible en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

NOTA: Si modifica esta opción, el servidor se reiniciará cuando seleccione **Guardar** y **Salir** para aplicar la nueva configuración

Cancelación de servicios del sistema

Presione <Entrar> para seleccionar **No** o **Sí**.

Al seleccionar **Sí,** se cierran todas las sesiones de Unified Server Configurator y el servidor se reinicia al seleccionar **Guardar** y **Salir** para aplicar la nueva configuración.

Configuración de LCD

Presione <Entrar> para mostrar el submenú **Configuración de LCD**. Cuando haya terminado de configurar los parámetros de LCD, presione <Esc> para volver al menú anterior.

Tabla 18-2. Configuración de usuario de LCD

Línea 1de LCD	Presione la <Flecha derecha>, <Flecha izquierda > y la barra espaciadora para cambiar entre las opciones. Esta función configura la pantalla **Inicio** en la LCD para una de las siguientes opciones: **Temp. ambiente**, **Etiqueta de información**, **Nombre de host**, **Dirección IPv4 del iDRAC6**, **Dirección IPv6 del iDRAC6**, **Dirección MAC del iDRAC6**, **Número de modelo**, **Ninguno**, **Etiqueta de servicio, Alimentación del sistema**, **Cadena definida por el usuario.**
Cadena definida por el usuario para LCD	Si la **Línea 1 de LCD** se establece en **Cadena definida por el usuario**, vea o introduzca la cadena que se mostrará en la pantalla LCD. La cadena puede tener un máximo de 62 caracteres.
Unidades de alimentación del sistema para LCD	Si **Línea 1 de LCD** se establece en **Alimentación del sistema**, seleccione **Vatio** o **BTU/h** para especificar la unidad que se mostrará en la pantalla LCD.
Unidades de temperatura ambiente para LCD	Si **Línea 1 de LCD** se establece en **Temp.ambiente**, seleccione **Centígrado** o **Fahrenheit** para especificar la unidad que se mostrará en la pantalla LCD.
Pantalla de error de LCD	Seleccione **Simple** o **SEL** (registro de eventos del sistema). Esta función permite que se muestren los mensajes de error en la pantalla LCD en uno de dos formatos: El formato simple provee una descripción del evento en idioma inglés. El formato SEL muestra una cadena de texto del registro de eventos del sistema.
Indicación de KVM remoto en LCD	Seleccione **Activado** para mostrar el texto*KVM* siempre que un KVM virtual esté activado en la unidad.
Acceso al panel anterior de LCD	Presione la <Flecha derecha>, <Flecha izquierda> y la barra espaciadora para cambiar entre las opciones: **Desactivado**, **Ver/Modificar** y **Sólo ver.** Esta configuración define el nivel de acceso del usuario para la pantalla LCD.

Configuración de usuario de LAN

El usuario de LAN es la cuenta de administrador del iDRAC, que tiene el nombre predeterminado **root**. Presione <Entrar> para mostrar el submenú de configuración de usuario de LAN. Cuando haya terminado de configurar el usuario de LAN, presione <Esc> para volver al menú anterior.

Tabla 18-3. Configuración de usuario de LAN

Elemento	Descripción
Acceso de cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione **Desactivado** para desactivar la cuenta de administrador.
Privilegio de cuenta	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Entrar> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Escriba la nueva contraseña para la cuenta de administrador. Los caracteres no aparecerán en la pantalla cuando usted los escriba.
Confirmar la contraseña	Escriba nuevamente la nueva contraseña para la cuenta de administrador. Si los caracteres que introduce no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparecerá un mensaje y usted deberá introducir nuevamente la contraseña.

Restablecer valores predeterminados

Use la opción de menú **Restablecer valores predeterminados** para restablecer todos los valores predeterminados de fábrica de las opciones de configuración del iDRAC6. Esto puede ser necesario, por ejemplo, cuando usted ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC6 a partir de los valores predeterminados.

Presione <Entrar> para seleccionar el elemento. Aparece el mensaje de advertencia siguiente:

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Continuar?

< NO (Cancelar) >

< SÍ (Continuar) >0
```

Seleccione **SÍ** y presione <Entrar> para restablecer los valores predeterminados del iDRAC.

Menú del registro de eventos del sistema

El menú **Registro de eventos del sistema** permite ver y borrar los mensajes del registro de eventos del sistema (SEL). Presione <Entrar> para mostrar el **Menú del registro de eventos del sistema**. El sistema cuenta las entradas del registro y después muestra el número total de entradas y el mensaje más reciente. El SEL retiene un máximo de 512 mensajes.

Para ver los mensajes del SEL, seleccione **Ver registro de eventos del sistema** y presione <Entrar>. Use la <Flecha izquierda> para retroceder al mensaje anterior (más antiguo) y la <Flecha derecha> para avanzar al mensaje siguiente (más reciente). Introduzca un número de registro para ir directamente al registro. Presione <Esc> cuando haya terminado de ver los mensajes del SEL.

Para borrar el SEL, seleccione **Borrar el registro de eventos del sistema** y presione <Entrar>.

Cuando haya terminado con el menú del SEL, presione <Esc> para volver al menú anterior.

Cómo salir de la utilidad de configuración del iDRAC

Cuando haya terminado de hacer cambios en la configuración del iDRAC, presione la tecla <Esc> para mostrar el menú de salida.

Seleccione **Guardar cambios y salir** y presione <Entrar> para retener los cambios.

Seleccione **Descartar cambios y salir** y presione <Entrar> para ignorar los cambios que ha realizado.

Seleccione **Regresar a la configuración** y presione <Entrar> para volver a la utilidad de configuración del iDRAC.

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alertas

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

En esta sección se explica cómo supervisar el iDRAC6 y se describen los procedimientos para configurar el sistema y el iDRAC6 para recibir alertas.

Configuración del sistema administrado para capturar la pantalla de último bloqueo

Antes de que el iDRAC6 pueda capturar la pantalla de último bloqueo, se debe configurar el sistema administrado con los siguientes prerrequisitos.

1. Instale el software del sistema administrado. Para obtener más información sobre la instalación del software del sistema administrado, consulte la *Guía del usuario de Server Administrator*.

2. Ejecute un sistema operativo admitido Microsoft® Windows® con la función de "reinicio automático" de Windows deseleccionada en la **Configuración de inicio y recuperación de Windows**.

3. Active la pantalla de último bloqueo (desactivada de manera predeterminada).

   Para activarla por medio de RACADM local, abra una petición de comandos y escriba los comandos siguientes:

   ```
   racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
   ```

4. Active el temporizador de recuperación automática y defina la acción **Recuperación automática** como **Restablecer**, **Apagar** o **Ciclo de encendido**. Para configurar el temporizador de **Recuperación automática**, debe usar Server Administrator o IT Assistant.

   Para obtener información sobre cómo configurar el temporizador de **Recuperación automática**, consulte la *Guía del usuario de Server Administrator*. Para garantizar que se pueda capturar la pantalla de último bloqueo, el temporizador de **Recuperación automática** se debe establecer en 60 segundos o más. El valor predeterminado es de 480 segundos.

   La pantalla de último bloqueo no está disponible cuando la acción **Recuperación automática** se establece como **Apagar** o **Ciclo de encendido** si el sistema administrado está bloqueado.

Desactivación de la opción de reinicio automático de Windows

Para asegurarse de que la función de pantalla de último bloqueo de la interfaz web del iDRAC6 funcione correctamente, se debe desactivar la opción **Reinicio automático** en los sistemas administrados que ejecutan los sistemas operativos Microsoft Windows® Server 2008 y Windows Server 2003.

Desactivación de la opción de reinicio automático en Windows 2008 Server

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.

2. Haga clic en Configuración **Avanzada del Sistema** bajo **Tareas** en la izquierda.

3. Haga clic en la lengüeta **Opciones avanzadas**.

4. En **Inicio y recuperación**, haga clic en **Configuración**.

5. Deseleccione la casilla **Reiniciar automáticamente**.

6. Haga clic dos veces en **Aceptar**.

Desactivación de la opción de reinicio automático en Windows Server 2003

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.

2. Haga clic en la lengüeta **Opciones avanzadas**.

3. En **Inicio y recuperación**, haga clic en **Configuración**.

4. Deseleccione la casilla **Reiniciar automáticamente**.

5. Haga clic dos veces en **Aceptar**.

Configuración de los eventos de plataforma

La configuración de eventos de plataforma tiene un mecanismo para configurar el dispositivo de acceso remoto a fin de realizar las acciones seleccionadas ante ciertos mensajes de eventos. Estas acciones incluyen reiniciar, ciclo de encendido, apagar y enviar una alerta (excepción de eventos de plataforma [PET] y/o por correo electrónico).

Los eventos de plataforma que se pueden filtrar incluyen los siguientes:

- Filtro de declaración crítica del ventilador
- Filtro de declaración de advertencia de la batería
- Filtro de declaración crítica de la batería
- Filtro de declaración crítica de voltaje discreto
- Filtro de declaración de advertencia de temperatura
- Filtro de declaración crítica de temperatura
- Filtro de declaración crítica de intrusión
- Filtro degradado de redundancia
- Filtro de pérdida de redundancia
- Filtro de declaración de advertencia del procesador
- Filtro de declaración crítica del procesador
- Filtro de ausencia del procesador
- Filtro de declaración de advertencia del suministro del procesador
- Filtro de declaración crítica del suministro del procesador
- Filtro de declaración de ausencia del suministro del procesador
- Declaración crítica de registro de eventos
- Filtro de declaración crítica de vigilancia
- Filtro de declaración de advertencia de alimentación del sistema
- Filtro de declaración crítica de alimentación del sistema

Cuando se presenta un evento de plataforma (por ejemplo, una falla de la sonda de ventilador), el evento se genera y se registra en el registro de eventos del sistema (SEL). Si este evento coincide con un filtro de eventos de plataforma (PEF) en la lista de filtros de eventos de plataforma de la interfaz web y usted ha configurado este filtro para que genere una alerta (PET o por correo electrónico), se enviará una alerta de PET o por correo electrónico a un conjunto de uno o más destinos configurados.

Si el mismo filtro de eventos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecutará.

Configuración de los filtros de eventos de plataforma (PEF)

Configure los filtros de eventos de plataforma antes de configurar excepciones de eventos de plataforma o alertas por correo electrónico.

Configuración de PEF por medio de la interfaz web

Para obtener más información, consulte "Configuración de los filtros de eventos de plataforma (PEF)".

Configuración de PEF por medio de la interfaz de línea de comandos de RACADM

1. Active el PEF.

   Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   donde `1` y `1` son el índice de PEF y la selección de activación/desactivación, respectivamente.

   El índice de PEF puede ser un valor de 1 a 19 La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar un PEF con índice 5, escriba el comando siguiente:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. Configure las acciones de PEF.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <acción>
   ```

   donde los bits de los valores *<acción>* son los siguientes:

   - 0 = sin acción de alerta
   - 1 = apagar servidor
   - 2 = reiniciar servidor
   - 3 = realizar ciclo de encendido del servidor

   Por ejemplo, para hacer que el PEF reinicie el sistema, escriba el siguiente comando:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   donde `1` es el índice de PEF y 2 es la acción del PEF de reiniciar.

Configuración de la PET

Configuración de la PET por medio de la interfaz web de usuario

Para obtener más información, consulte "Configuración de excepciones de eventos de plataforma (PET)".

Configuración de PET por medio de la interfaz de línea de comandos de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active la PET.

   En la petición de comandos, escriba los comandos siguientes y presione <Entrar> después de cada uno:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   ```
   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   donde `1` y `1` son el índice de destino de PET y la selección de activación/desactivación, respectivamente.

   El índice de destino de PET puede ser un valor de 1 a 4. La selección de activación o desactivación puede ser 1 (activado) o 0 (desactivado).

   Por ejemplo, para activar una PET con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

   ```
   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 4 1
   ```

3. Configure la política de PET.

   En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

   ```
   iPv4:racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <dirección_IPv4>
   ```

   ```
   iPv6:racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 <dirección_IPv6>
   ```

   donde `1` es el índice de destino de la PET y *<dirección_IPv4>* y *<dirección_IPv6>* son los destinos de direcciones IP del sistema que recibe las alertas de eventos de plataforma.

4. Configure la cadena de nombre de comunidad.

   En la petición de comandos, escriba:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Nombre>
   ```

Configuración de alertas por correo electrónico

Configuración de alertas por correo electrónico por medio de la interfaz web de usuario

Para obtener más información, consulte "Configuración de alertas por correo electrónico".

Configuración de alertas por correo electrónico por medio de la interfaz de línea de comandos de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico.

   En el indicador de comandos, escriba los siguientes comandos y pulse <Entrar> después de cada uno:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   donde `1` y `1` son el índice de destino de correo electrónico y la selección de activación/desactivación, respectivamente.

   El índice de destino de correo electrónico puede ser un valor de 1 a 4. La selección de activación o desactivación puede ser 1 (activado) o 0 (desactivado).

   Por ejemplo, para activar un correo electrónico con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configure los valores del correo electrónico.

   En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>`

   donde `1` es el índice de destino de correo electrónico y *<dirección_de_correo_electrónico>* es la dirección de correo electrónico de destino que recibe las alertas de eventos de plataforma.

   Para configurar un mensaje personalizado, en la petición de comandos escriba el comando siguiente y presione <Entrar>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <mensaje_personalizado>`

   donde `1` es el índice de destino de correo electrónico y *<mensaje_personalizado>* es el mensaje que se muestra en la alerta por correo electrónico.

Pruebas de las alertas por correo electrónico

La función de alertas por correo electrónico del RAC permite que los usuarios reciban alertas por correo electrónico cuando se presenta un evento crítico en el sistema administrado. El ejemplo a continuación muestra cómo probar la función de envío de alertas por correo electrónico para garantizar que el RAC pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Compruebe que los valores de **SMTP** y **Alerta por correo electrónico** estén configurados antes de probar la función de envío de alertas por correo electrónico. Consulte "Configuración de alertas por correo electrónico" para obtener más información.

Comprobación de la función de alertas de excepción SNMP del RAC

La función de alertas de excepción SNMP del RAC permite que las configuraciones del detector de excepciones SNMP reciban las excepciones para sucesos de sistema que se presenten en el sistema administrado.

El siguiente ejemplo muestra la manera en la que un usuario puede probar la función de alertas de excepciones SNMP del RAC.

```
racadm testtrap -i 2
```

Antes de probar la función de alertas de excepciones SNMP del RAC, asegúrese de que los valores de excepción y SNMP estén configurados correctamente. Consulte las descripciones de los subcomandos "**testtrap**" y "**sslkeyupload**" para configurar estos valores.

Preguntas frecuentes sobre la autenticación de SNMP

¿Por qué aparece el siguiente mensaje?

`Remote Access: SNMP Authentication Failure (Acceso remoto: error de autenticación de SNMP)`

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad Get y Set del dispositivo. En IT Assistant, usted tiene el **nombre de comunidad Get = public** y el **nombre de comunidad Set = private.** De manera predeterminada, el nombre de comunidad para el agente iDRAC6 es **público**. Cuando IT Assistant envía una solicitud Set, el agente iDRAC6 genera el error de autenticación SNMP porque sólo acepta solicitudes de **comunidad = public (público)**.

NOTA: Este nombre de comunidad de agente SNMP se utiliza para descubrimiento.

Puede cambiar el nombre de comunidad del iDRAC6 por medio de RACADM.

Para ver el nombre de comunidad del iDRAC6, use el comando siguiente:

```
racadm getconfig -g cfgOobSnmp
```

Para establecer el nombre de comunidad del iDRAC6, use el comando siguiente:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nombre de comunidad>
```

Para acceder al nombre de comunidad de agente SNMP del iDRAC6 o configurarlo, utilice la interfaz web, diríjase a **Acceso Remoto**→ **Configuración**→ **Servicios** y haga clic en **Agente SNMP.**

Para evitar que se generen errores de autenticación de SNMP, se deben introducir nombres de comunidad que el agente acepte. Como el iDRAC6 sólo permite un nombre de comunidad, se debe usar el mismo nombre de comunidad **get** y **set** para la configuración de descubrimiento de IT Assistant.

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del sistema administrado

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección explica cómo realizar tareas relacionadas con la recuperación y solución de problemas de un sistema remoto bloqueado mediante la interfaz web del iDRAC6.

- "Primeros pasos para solucionar problemas de un sistema remoto"
- "Administración de energía en un sistema remoto"
- "Información IPv6"
- "Cómo ver la pantalla de último bloqueo del sistema"

Primeros pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas de alto nivel en el sistema administrado:

1. ¿El sistema está encendido o apagado?
2. Si está encendido, ¿el sistema operativo se encuentra en funcionamiento, bloqueado o simplemente congelado?
3. Si está apagado, ¿se ha apagado de forma imprevista?

En el caso de sistemas bloqueados, revise la pantalla de último bloqueo (consulte "Cómo ver la pantalla de último bloqueo del sistema") y use la redirección de consola y la administración remota de energía (consulte "Administración de energía en un sistema remoto") para reiniciar el sistema y observar el proceso de reinicio.

Administración de energía en un sistema remoto

El iDRAC6 permite realizar varias acciones de administración de energía de forma remota en el sistema administrado para que se pueda recuperar después de un bloqueo o de algún otro evento del sistema.

Seleccione Acciones de control de alimentación de la interfaz web del iDRAC6.

Para realizar acciones de administración de energía mediante la interfaz web, consulte "Ejecución de operaciones de control de alimentación en el servidor".

Selección de las acciones de control de alimentación desde la interfaz de línea de comandos del iDRAC6

Use el comando `racadm serveraction` para realizar operaciones de administración de energía en el sistema host.

```
racadm serveraction <acción>
```

Las opciones para la cadena <*acción*> son:

- **powerdown**: apaga el sistema administrado.
- **powerup**: enciende el sistema administrado.
- **powercycle**: ejecuta una operación de ciclo de encendido en el sistema administrado. Esta acción es similar a presionar el botón de encendido en el panel anterior del sistema para apagarlo y después encender el sistema.
- **powerstatus**: muestra el estado actual de la alimentación del servidor ("Encendido" o "Apagado")
- **hardreset**: ejecuta una operación de restablecimiento (reinicio) en el sistema administrado.

Cómo ver la información del sistema

La página **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Chasis del sistema principal
- Integrated Dell Remote Access Controller 6 - Enterprise

Para acceder a la información del sistema, amplíe el árbol **Sistema** y haga clic en **Propiedades**.

Chasis del sistema principal

La Tabla 20-1 y la Tabla 20-2 describen las propiedades del chasis de sistema principal.

NOTA: Para recibir la información del **Nombre de host** y el **Nombre del sistema operativo**, deberá tener instalados los servicios del iDRAC6 en el sistema administrado.

Tabla 20-1. Campos de la información del sistema

Campo	Descripción
Descripción	Descripción del sistema.
Versión del BIOS	Versión del BIOS del sistema.
Etiqueta de servicio	Número de la etiqueta de servicio del sistema.
Nombre de host	Nombre del sistema host.
Nombre del sistema operativo	El sistema operativo que se ejecuta en el sistema.

Tabla 20-2. Campos de la recuperación automática

Campo	Descripción
Acción de recuperación	Cuando se detecta un "sistema bloqueado", se puede configurar el iDRAC6 para que ejecute una de las siguientes acciones: sin acción, restablecimiento forzado, apagar o realizar ciclo de encendido del sistema.
Cuenta regresiva inicial	El número de segundos tras la detección de un "sistema bloqueado" después de los cuales el iDRAC6 ejecutará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Integrated Dell Remote Access Controller 6 Enterprise

La Tabla 20-3 describe las propiedades de iDRAC6 Enterprise

Tabla 20-3. Campos de información de iDRAC6 Enterprise

Campo	Descripción
Fecha/Hora	Tiempo actual en la forma: Día Mes DD HH:MM:SS:AAAA
Versión del firmware	Versión del firmware del iDRAC
Firmware actualizado	La fecha del firmware fue mostrada en la forma: Día Mes DD HH:MM:SS:AAAA
Versión del hardware	Versión del controlador de acceso remoto.
Dirección MAC	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red.

Información IPv4

La Tabla 20-4 describe las propiedades IPv4

Tabla 20-4. Campos de información IPv4

Campo	Descripción
Activado	Sí o No
Dirección IP	La dirección de 32 bits que identifica la tarjeta de interfaz de red (NIC) a un host. El valor se muestra en formato de números separados

	con puntos, por ejemplo, 143.166.154.127.
Máscara de subred	La máscara de subred identifica las partes de la dirección IP que forman el prefijo extendido de red y el número de host. El valor se muestra en formato de números separados con puntos, por ejemplo, 255.255.0.0.
Puerta de enlace	Dirección de un router o un conmutador. El valor se muestra en formato de números separados con puntos, por ejemplo, 143.166.154.127.
DHCP activado	Sí o No. Indica si el protocolo de configuración dinámica de host (DHCP) está activado.

Información IPv6

La Tabla 20-5 describe las propiedades IPv6.

Tabla 20-5. Campos de información IPv6

Campo	Descripción
Activado	Indica si la pila IPv6 está activada.
Dirección IP 1	Especifica la dirección IPv6 de la NIC del iDRAC6.
Longitud del prefijo	Número entero que especifica la longitud del prefijo de la dirección IPv6. Se puede valuar entre 1 y 128 inclusive.
Puerta de enlace IP	Especifica la puerta de enlace de la NIC del iDRAC6.
Dirección local de vínculo	Especifica la dirección IPv6 de la NIC del iDRAC6.
Dirección IP 2	Especifica la dirección IPv6 adicional de la NIC del iDRAC6, si hay una disponible.
Auto Config	AutoConfig permite que Server Administrator obtenga la dirección IPv6 para la NIC del iDRAC del servidor del protocolo de configuración dinámica de host (DHCPv6). Además, desactiva y hace salir los valores de dirección IP estática, longitud del prefijo y puerta de enlace.

Uso del registro de eventos del sistema (SEL)

La página **SEL** muestra los eventos críticos del sistema que se presentan en el sistema administrado.

Para ver el registro de eventos del sistema:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la lengüeta **Registros** y después haga clic en **Registro de eventos del sistema**.

   La página **Registro de eventos del sistema** muestra la gravedad del evento y ofrece otra información según se muestra en la Tabla 20-6.
3. Haga clic en el botón correspondiente de la página **Registro de eventos del sistema** para continuar (consulte la Tabla 20-6).

Tabla 20-6. Iconos de indicador de estado

Icono/categoría	Descripción
	Una marca de verificación verde indica una condición de estado correcta (normal).
	Un triángulo amarillo que contiene un signo de admiración indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.
Fecha/Hora	La fecha y hora en la que se presentó el evento. Si la fecha está en blanco, el evento se presentó durante el inicio del sistema. El formato es mm/dd/aaaa hh:mm:ss, según el horario de 24 horas.
Descripción	Una breve descripción del evento

Tabla 20-7. Botones de la página SEL

Botón	Acción
Imprimir	Imprime el **registro de eventos del sistema en el orden en que aparece en la ventana**.
Actualizar	Vuelve a cargar la página **SEL**.
Borrar registro	Borra el **registro de eventos del sistema**. **NOTA:** El botón **Borrar registro** sólo aparece si usted tiene permiso para **Borrar registros**.

Guardar como	Abre una ventana emergente que le permite guardar el **registro de eventos del sistema** en el directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en support.microsoft.com.

Uso de la línea de comandos para ver el registro del sistema

```
racadm getsel -i
```

El comando **getsel -i** muestra el número de entradas en el registro de eventos del sistema.

```
racadm getsel <opciones>
```

NOTA: Si no se especifican argumentos, se mostrará todo el registro.

NOTA: Consulte "getsel" para obtener más información sobre las opciones que puede usar.

El comando **clrsel** elimina todos los registros existentes del registro de eventos del sistema.

```
racadm clrsel
```

Uso de los registros de inicio del POST (Power- On Self-Test [autoprueba de encendido])

NOTA: Todos los registros son eliminados después de que se reinicia el iDRAC6.

Esta función del iDRAC6 le permite reproducir un vídeo de imágenes detenidas de las últimas tres instancias de la prueba POST del BIOS.

Para ver los registros de capturas de inicio de POST:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la lengüeta **Registros** y luego en la lengüeta **Captura de INICIO**.
3. Seleccione el número de registro de captura de inicio de POST y haga clic en **Reproducir**.

   El vídeo de los registros se reproducirá en una nueva pantalla.

   NOTA: Debe cerrar el vídeo abierto de captura de inicio de POST antes de reproducir otro. No puede reproducir dos registros simultáneamente.
4. Haga clic en **Reproducción**→ **Reproducir** para comenzar el vídeo de captura de inicio de POST.
5. Haga clic en **DETENER** para detener el vídeo.

La tarjeta iDRAC6 Express es vinculada al iDRAC6 cuando se accede a la aplicación Unified Server Configurator (USC) al presionar **F10** durante el inicio. Si el vínculo se establece correctamente, se registra el siguiente mensaje en el registro de eventos del sistema y la pantalla LCD: `La iDRAC6 Upgrade Successful (actualización del iDRAC6 se realizó con éxito)`. Si falla, se registra el siguiente mensaje: iDRAC6 `Upgrade Failed (La actualización del iDRAC6 no pudo realizarse)`. Aun más, cuando una tarjeta iDRAC6 Express con un firmware de iDRAC6 anterior o desactualizado que no admite una plataforma específica se inserta en la placa base y el sistema se inicia, se genera un registro en la pantalla de POST que indica: `iDRAC firmware is out-of-date. Please update to the latest firmware (El firmware del iDRAC está desactualizado. Actualice el firmware a la versión más reciente)`. Actualice la tarjeta iDRAC6 Express con la versión más reciente del firmware del iDRAC6 para la plataforma específica. Para obtener más información, consulte la Guía del usuario de *Dell Unified Server Configurator y Dell Unified Server Configurator– Lifecycle Controller Enabled*.

Cómo ver la pantalla de último bloqueo del sistema

NOTA: La función de pantalla de último bloqueo necesita que el sistema administrado tenga configurada la función **Recuperación automática** en Server Administrator. Además, asegúrese de que la función **Recuperación automática del sistema** esté activada por medio del iDRAC6. Diríjase a la página **Servicios** en la lengüeta **Configuración** en la sección **Acceso remoto** para activar esta función.

La página **Pantalla de último bloqueo** muestra la más reciente pantalla del último bloqueo del sistema. La información del último bloqueo se guarda en la memoria del iDRAC6 y se puede acceder a ella de manera remota.

Para ver la página **Pantalla de último bloqueo**:

1. En el árbol **Sistema**, haga clic en **Sistema**.

2. Haga clic en la lengüeta **Registros** y después haga clic en **Pantalla de último bloqueo**.

La página **Pantalla de último bloqueo** tiene los siguientes botones (consulte la Tabla 20-8) en la esquina superior derecha de la pantalla:

Tabla 20-8. Botones de la página Pantalla de último bloqueo

Botón	Acción
Imprimir	Imprime la página **Pantalla de último bloqueo**.
Actualizar	Vuelve a cargar la página **Pantalla de último bloqueo**.

NOTA: Debido a fluctuaciones en el temporizador de recuperación automática, es posible que la **Pantalla de último bloqueo** no se capture cuando el temporizador de restablecimiento del sistema esté definido con un valor de menos de 30 segundos. Utilice Server Administrator o IT Assistant para establecer el valor del temporizador de restablecimiento del sistema en al menos 30 segundos y garantizar que la **Pantalla de último bloqueo** funcione correctamente. Para obtener información adicional, consulte "Configuración del sistema administrado para capturar la pantalla de último bloqueo".

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del iDRAC6

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Esta sección explica cómo realizar las tareas relacionadas con la recuperación y solución de problemas de un iDRAC6 bloqueado.

Usted puede usar una de las siguientes herramientas para solucionar problemas del iDRAC6.

- Registro del RAC.
- Consola de diagnósticos
- Registro de rastreo
- racdump
- coredump

Uso del registro del RAC

El **Registro del RAC** es un registro persistente que se mantiene en el firmware del iDRAC6. El registro contiene una lista de las acciones de usuario (como inicio y cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC6.. Cuando el registro se llena, las entradas más antiguas se sobrescriben.

Para acceder al registro del RAC desde la interfaz de usuario del iDRAC6:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Registros** y después haga clic en **Registro del RAC**.

El **Registro del RAC** proporciona la información que aparece en la Tabla 21-1.

Tabla 21-1. Información de la página del registro del RAC

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 de dic. 16:55:47). Cuando el iDRAC6 se inicia por primera vez y no se puede comunicar con el sistema administrado, la hora se muestra como System Boot (Inicio del sistema).
Origen	La interfaz que ocasionó el evento.
Descripción	Una breve descripción del evento y el nombre de usuario que inició sesión en el iDRAC6.

Uso de los botones de la página de registro del RAC

La página **Registro del RAC** tiene los botones que aparecen en la Tabla 21-2.

Tabla 21-2. Botones del registro del RAC

Botón	Acción
Imprimir	Imprime la página **Registro del RAC**.
Borrar registro	Borra las entradas del **Registro del RAC**. **NOTA:** El botón **Borrar registro** sólo aparece si usted tiene permiso para **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **Registro del RAC** en un directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en **support.microsoft.com**.

Actualizar	Vuelve a cargar la página **Registro del RAC**.

Utilización de la línea de comandos

Utilice el comando `getraclog` para ver las entradas del registro del RAC.

```
racadm getraclog -i
```

El comando **getraclog -i** muestra el número de entradas en el registro de iDRAC6.

```
racadm getraclog [opciones]
```

NOTA: Para obtener más información, consulte "getraclog".

Puede usar el comando `clrraclog` para borrar todas las entradas del registro del RAC.

```
racadm clrraclog
```

Uso de la consola de diagnósticos

El iDRAC6 proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la Tabla 21-3) que son similares a las herramientas que se incluyen con los sistemas con Microsoft® Windows® o Linux. Por medio de la interfaz web del iDRAC6 se puede acceder a las herramientas de depuración de red.

Para acceder a la página de **Consola de diagnósticos**:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Diagnósticos**.

La Tabla 21-3 describe las opciones que están disponibles en la página **Consola de diagnósticos**. Escriba un comando y haga clic en **Enviar**. Los resultados de depuración aparecen en la página **Consola de diagnósticos**.

Para actualizar la página **Consola de diagnósticos**, haga clic en **Actualizar**. Para ejecutar otro comando, haga clic en **Volver a la página de diagnósticos**.

Tabla 21-3. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las entradas del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
netstat	Imprime el contenido de la tabla de encaminamiento. Si se proporciona el número de interfaz opcional en el campo de texto situado a la derecha de la opción **netstat**, dicha opción imprimirá información adicional acerca del tráfico en la interfaz, uso de búfer y otra información de interfaz de red.
ping *<Dirección IP>*	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de encaminamiento. Se debe introducir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de encaminamiento actual.
gettracelog	Muestra el registro de rastreo del iDRAC6. Consulte "gettracelog" para obtener más información.

Uso del registro de rastreo

El registro de rastreo del iDRAC6 es utilizado por los administradores para depurar las alertas del iDRAC6 y los problemas del sistema de red.

Para acceder al registro de rastreo desde la interfaz web del iDRAC6:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Diagnósticos**.
3. En el campo **Comando**, escriba el comando **gettracelog** o el comando **racadm gettracelog**.

   NOTA: También puede usar este comando en la interfaz de línea de comandos. Para obtener más información, consulte "gettracelog".

El registro de rastreo recopila la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben del mismo.

- IP: rastrea los paquetes IP que se envían y reciben.

El registro de rastreo también puede contener códigos de error específicos del firmware del iDRAC6 que están relacionados con el firmware interno del iDRAC6, no con el sistema operativo del sistema administrado.

NOTA: El iDRAC6 no generará un eco para un ICMP (ping) con un tamaño de paquete mayor de 1500 bytes.

Uso de racdump

El comando **racadm racdump** proporciona un sólo comando para obtener información sobre volcado, estado e información general sobre la tarjeta del iDRAC6

NOTA: Este comando sólo está disponible en las interfaces Telnet y SSH. Para obtener más información, consulte el comando "racdump".

Uso de coredump

El comando **racadm coredump** muestra información detallada sobre los problemas críticos recientes que se hayan presentado en el RAC. La información de volcado de núcleo se puede usar para diagnosticar estos problemas críticos.

Si está disponible, la información de volcado de núcleo permanece después de ciclos de encendido del RAC y seguirá disponible hasta que se presente alguna de las condiciones siguientes:

- La información de volcado de núcleo se borra con el subcomando **coredumpdelete**.
- Se presenta otra condición crítica en el RAC. En este caso, la información de volcado de núcleo se referirá al último error crítico que se haya presentado.

El comando racadm coredumpdelete puede usarse para borrar los datos de **volcado de núcleo** que residan en ese momento en el RAC.

Consulte los subcomandos "coredump" y "coredumpdelete" para obtener más información.

Regresar a la página de contenido

Regresar a la página de contenido

Sensores

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

Las sondas o sensores de hardware ayudan a supervisar los sistemas de la red de manera más eficiente, ya que permiten tomar las medidas apropiadas para evitar que se produzcan problemas tales como la inestabilidad o daños del sistema.

El iDRAC6 puede utilizarse para supervisar los sensores de hardware de baterías, sondas de ventiladores, intrusión en el chasis, suministros de energía, consumo de energía, temperatura y voltajes.

Sondas de baterías

Las sondas de baterías brindan información sobre el CMOS de la placa base y la RAM de almacenamiento en baterías de la placa base (ROMB).

NOTA: La configuración de las baterías de ROMB de almacenamiento sólo se encuentra disponible si el sistema tiene ROMB.

Sondas de ventiladores

Los sensores de sondas de ventiladores ofrecen la siguiente información:

- redundancia del ventilador: indica la capacidad del ventilador secundario de reemplazar al principal si no logra disipar el calor a una velocidad preestablecida.
- lista de sondas de ventiladores: la lista ofrece información sobre la velocidad de todos los ventiladores del sistema.

Sondas de intrusión en el chasis

Las sondas de intrusión en el chasis indican el estado del chasis, ya sea abierto o cerrado.

Sondas de suministros de energía

Las sondas de suministros de energía brindan la siguiente información:

- Estado del suministro de energía
- La redundancia del suministro de energía, es decir, la capacidad del suministro de energía redundante de reemplazar al suministro principal en caso de falla.

NOTA: Si sólo existe un suministro de energía en el sistema, la redundancia de suministro de energía quedará **desactivada**.

Sondas de supervisión de la alimentación

La supervisión de la alimentación brinda información sobre el consumo de energía en *tiempo real*, en vatios y amperios.

También es posible ver una representación gráfica del consumo de energía del último minuto, hora, día o semana a partir de la hora actual definida en el iDRAC6.

Sonda de temperatura

El sensor de temperatura brinda información sobre la temperatura ambiente de la placa base. La sonda de temperatura indica si el estado de la sonda se encuentra dentro del umbral crítico y de advertencia preestablecido.

Sondas de voltaje

A continuación se enumeran las sondas de voltaje de uso habitual. Su sistema puede tener éstas y/u otras sondas.

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

Las sondas de voltaje indican si el estado de la sonda se encuentra dentro de los valores de umbral crítico y de advertencia preestablecidos.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de las funciones de seguridad

Guía del usuario de Integrated Dell™ Remote Access Controller 6 (iDRAC6) versión 1.1

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Opciones de seguridad avanzada para el administrador del iDRAC6:
  - La opción de desactivación de la redirección de consola permite que el usuario *local* del sistema desactive la redirección de consola por medio de la función de redirección de consola del iDRAC6.
  - Las funciones de desactivación de la configuración local permiten que el administrador del iDRAC6 *remoto* desactive de manera selectiva la capacidad de configurar el iDRAC6 a partir de:
    - La ROM de opción de la POST del BIOS
    - El sistema operativo que usa RACADM local y las utilidades de Dell™ OpenManage™ Server Administrator
- La operación de la interfaz web y la interfaz de línea de comandos de RACADM, que admite el cifrado SSL de 128 bits y el cifrado SSL de 40 bits (para los países en los que no se acepta el cifrado de 128 bits)

  NOTA: Telnet no admite el cifrado SSL.

- Configuración de la expiración de tiempo de la sesión (en segundos) mediante la interfaz web o la interfaz de línea de comandos de RACADM
- Puertos IP que se pueden configurar (en los casos correspondientes)
- Secure Shell (SSH), que utiliza una capa cifrada de transporte para brindar una mayor seguridad.
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.
- Rango limitado de direcciones IP para clientes que se conectan al iDRAC6

Opciones de seguridad avanzada para el administrador del iDRAC6

Desactivar la configuración local del iDRAC6

Los administradores pueden desactivar la configuración local por medio de la interfaz gráfica del usuario (GUI) del iDRAC6 al seleccionar **Acceso remoto**→ **Configuración**→ **Servicios**. Cuando se selecciona la casilla **Desactivar la configuración local del iDRAC por medio de la ROM de opción**, la utilidad de configuración del iDRAC6 (a la que se accede al presionar <Ctrl+E> durante el inicio del sistema) funciona en modo de sólo lectura, lo que evita que los usuarios locales puedan configurar el dispositivo. Cuando el administrador selecciona la casilla **Desactivar la configuración local del iDRAC por medio de RACADM**, los usuarios locales no pueden configurar el iDRAC6 por medio de la utilidad RACADM ni Dell OpenManage Server Administrator, pero aún pueden leer los valores de configuración.

Los administradores pueden activar una de estas opciones al mismo tiempo o ambas. Además de activarlas por medio de la interfaz gráfica del usuario, los administradores también pueden utilizar los comandos locales de RACADM.

Desactivación de la configuración local durante el reinicio del sistema

Esta función desactiva la capacidad que tiene el usuario del sistema administrado de configurar el iDRAC6 durante el reinicio del sistema.

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

NOTA: Esta opción se admite sólo en la utilidad de configuración del iDRAC6. Para actualizarse con esta versión, actualice el BIOS por medio del paquete de actualización del BIOS que se encuentra sitio web de asistencia de Dell en **support.dell.com**.

Desactivación de la configuración local a partir de RACADM local

Esta función desactiva la capacidad del usuario del sistema administrado de configurar el iDRAC6 por medio de las utilidades de RACADM local o de Dell OpenManage Server Administrator.

```
racadm config -g cfgRacTuning -o cfgRacTuneConRedirEncryptEnable 1
```

PRECAUCIÓN: Estas funciones limitan en gran medida la capacidad del usuario local para configurar el iDRAC6 desde el sistema local, lo que incluye el restablecimiento de la configuración predeterminada. Dell recomienda que se utilicen estas funciones a discreción y se debe desactivar

sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión.

NOTA: Para obtener más información, consulte el documento técnico *Desactivación de la configuración local y el KVM virtual remoto en el DRAC* en el sitio web de asistencia de Dell en **support.dell.com**.

Aunque los administradores pueden establecer las opciones de configuración local por medio de los comandos de racadm local, por motivos de seguridad sólo pueden restablecerlos a partir de una interfaz de línea de comandos o una interfaz web del iDRAC6 fuera de banda. La opción `cfgRacTuneLocalConfigDisable` se aplica después de que la autoprueba de encendido del sistema ha terminado y el sistema ha terminado de iniciar el entorno de sistema operativo. El sistema operativo puede ser un sistema tal como Microsoft® Windows Server® o Enterprise Linux que pueda ejecutar localmente comandos de racadm, o bien un sistema operativo de uso limitado tal como el Entorno de Preinstalación de Microsoft Windows® o vmlinux, utilizado para ejecutar los comandos de racadm locales de Dell OpenManage Deployment Toolkit

Hay varias situaciones que pueden requerir que los administradores desactiven la configuración local. Por ejemplo, en un centro de datos con varios administradores para servidores y dispositivos de acceso remoto, es posible que los responsables de mantener las pilas de software de servidor no necesiten tener acceso administrativo a los dispositivos de acceso remoto. Asimismo, los técnicos pueden tener acceso físico a los servidores durante mantenimiento de rutina de sistemas —durante el cual pueden reiniciar los sistemas y acceder al BIOS protegido con contraseña— pero no deben tener la facultad de configurar los dispositivos de acceso remoto. En situaciones de este tipo, es recomendable que los administradores de dispositivos de acceso remoto desactiven la configuración local.

Los administradores deben tener presente que debido a que la desactivación de la configuración local limita en gran medida los privilegios de configuración local —incluso la capacidad de restablecer la configuración predeterminada del iDRAC6— sólo deben utilizar estas opciones cuando sea necesario y normalmente deberán desactivar sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión. Por ejemplo, si los administradores han deshabilitado a todos los usuarios locales del iDRAC6 y sólo permiten que los usuarios del servicio de directorio Microsoft Active Directory® inicien sesión en el iDRAC6, y posteriormente falla la infraestructura de autenticación de Active Directory, es posible que los administradores no puedan iniciar sesión. Asimismo, si los administradores han desactivado toda la configuración local e incorporan un iDRAC6 con una dirección IP estática a una red que ya incluye un servidor de protocolo de configuración de host dinámico (DHCP), y éste luego asigna la dirección IP del iDRAC6 a otro dispositivo de la red, debido al conflicto resultante existe la posibilidad de que se desactive la conectividad fuera de banda del DRAC, lo que obliga a los administradores a restablecer la configuración predeterminada del firmware por medio de una conexión serie.

Desactivación del KVM virtual remoto del iDRAC6

Los administradores pueden desactivar de manera selectiva el KVM remoto del iDRAC6, lo que brinda un mecanismo seguro y flexible para que el usuario local trabaje en el sistema sin que alguien más vea las acciones del usuario a través de la redirección de consola. El uso de esta función requiere la instalación del software de nodo administrado de iDRAC en el servidor. Los administradores pueden desactivar el vKVM remoto con el siguiente comando:

```
racadm LocalConRedirDisable 1
```

El comando LocalConRedirDisable desactiva las ventanas de sesión vKVM remota existentes cuando se ejecuta con el argumento 1

Para ayudar a evitar que el usuario remoto anule la configuración del usuario local, este comando sólo está disponible para RACADM local. Los administradores pueden usar este comando en los sistemas operativos que admiten RACADM local, incluso en Microsoft Windows Server 2003 y SUSE Linux Enterprise Server 10. Como los efectos de este comando continúan después de reinicios del sistema, los administradores deben revertirlo específicamente para reactivar el vKVM remoto. Pueden hacer esto con el argumento 0:

```
racadm LocalConRedirDisable 0
```

Hay varias situaciones que pueden requerir la desactivación del vKVM remoto del iDRAC6. Por ejemplo, es posible que los administradores no deseen que un usuario del iDRAC6 remoto vea la configuración del BIOS que han establecido en un sistema, en tal caso, pueden desactivar el vKVM remoto durante la POST del sistema por medio del comando `LocalConRedirDisable`. Si también desean aumentar la seguridad a través de la desactivación automática del vKVM remoto cada vez que un administrador inicie sesión en el sistema, lo pueden hacer mediante la ejecución del comando `LocalConRedirDisable` en las secuencias de comandos de inicio de sesión del usuario.

NOTA: Para obtener más información, consulte el documento técnico *Desactivación de la configuración local y el KVM virtual remoto en el DRAC* en el sitio web de asistencia de Dell en **support.dell.com**.

Para obtener más información sobre las secuencias de comandos de inicio de sesión, consulte **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx.**

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales

Este apartado proporciona información acerca de las siguientes funciones de seguridad de datos que están incorporadas en el iDRAC6:

- "Capa de sockets seguros (SSL)"
- "Solicitud de firma de certificado (CSR)"
- "Acceso al menú principal de SSL"
- "Generación de una solicitud de firma de certificado"

Capa de sockets seguros (SSL)

El iDRAC6 incluye un servidor web que está configurado para usar el protocolo de seguridad SSL, que es el estándar de la industria, para transferir datos cifrados a través de Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas y es una técnica ampliamente aceptada para ofrecer comunicación cifrada y autenticada entre los clientes y servidores a fin de evitar intercepción furtiva a la información de la red.

Un sistema habilitado para SSL:

- Se autentica a sí mismo en un cliente habilitado para SSL

- Permite que el cliente se autentique a sí mismo en el servidor
- Permite que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado brinda una protección de datos de alto nivel. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está generalmente disponible para los exploradores de Internet en Norteamérica.

El servidor web del iDRAC6 incluye un certificado digital SSL firmado automáticamente de Dell (identificación de servidor). Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del servidor web mediante el envío de una solicitud al iDRAC6 para generar una nueva solicitud de firma de certificado (CSR).

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (CA) para obtener un certificado de servidor seguro. Los certificados de servidor seguro protegen la identidad de un sistema remoto y garantizan que otros usuarios no puedan ver o cambiar la información que se intercambia con dicho sistema. Para garantizar la seguridad del DRAC, se recomienda enfáticamente que se genere una CSR, se envíe a una autoridad de certificados y se cargue el certificado devuelto por la autoridad de certificados.

Una autoridad emisora de certificados es una entidad comercial que está reconocida por la industria de la tecnología informática por cumplir estándares altos de revisión confiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Después de recibir la solicitud CSR, la autoridad de certificados (CA) revisa y verifica la información que contiene. Si el candidato cumple los estándares de seguridad de la autoridad de certificados, ésta emite un certificado al candidato que lo identifica de forma exclusiva para transacciones a través de redes y en Internet.

Después de que la CA aprueba la CSR y le envía un certificado, se debe cargar el certificado en el firmware del iDRAC6 La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y haga clic en **SSL**.

Utilice el **Menú Principal de SSL** (vea la Tabla 23-1) para generar una CSR, cargar un certificado de servidor existente o ver un certificado de servidor existente. La información de la CSR se almacena en el firmware del iDRAC6. La Tabla 23-2 describe los botones disponibles en la página **SSL**.

Tabla 23-1. Menú principal de SSL

Campo	Descripción
Generar solicitud de firma de certificado (CSR)	Haga clic en **Siguiente** para abrir la página que permite generar una CSR para enviarla a una CA a fin de solicitar un certificado web seguro.
Cargar certificado de servidor	Haga clic en **Siguiente** para cargar un certificado existente sobre el que su compañía tenga derechos y que utiliza para controlar el acceso al iDRAC6. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509, base 64. No se aceptan los certificados codificados con DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su iDRAC6.
Ver el certificado de servidor	Haga clic en **Siguiente** para ver un certificado de servidor existente.

Tabla 23-2. Botones del menú principal de SSL

Botón	Descripción
Imprimir	Imprime la página **Menú principal de** SSL.
Actualizar	Vuelve a cargar la página **Menú principa**l de SSL.
Siguiente	Avanza a la página siguiente.

Generación de una solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que iDRAC acepte la CSR firmada, la CSR que está en el firmware debe coincidir con el certificado que CA devuelve.

1. En la página **Menú principal d**e SSL, seleccione **Generar solicitud de firma de certificado (CSR)** y haga clic en **Siguiente.**
2. En la página **Generar solicitud de firma de certificado (CSR)**, introduzca un valor para cada atributo de la CSR.

   La Tabla 23-3 describe las opciones de la página **Generar solicitud de firma de certificado (CSR)**.

3. Haga clic en **Generar** para abrir o guardar la CSR

4. Haga clic en el botón de la página **Generar solicitud de firma de certificado (CSR)** para continuar. La Tabla 23-4 describe los botones que están disponibles en la página **Generar solicitud de firma de certificado (CSR)**.

Tabla 23-3. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **www.empresaxyz.com**). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, espacios y puntos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad organizacional, como un departamento (por ejemplo, Grupo de empresa). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo o algún otro carácter.
Nombre del estado	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Texas). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación. Utilice el menú desplegable para seleccionar el país.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Puede escribir la dirección de correo electrónico de su empresa o cualquier dirección de correo electrónico que desee tener asociada con la CSR. Este campo es opcional.

Tabla 23-4. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime la página **Generar solicitud de firma de certificado (CSR)**.
Actualizar	Vuelve a cargar la página **Generar solicitud de firma de certificado (CSR)**.
Volver al menú principal de SSL	Regresa a la página **Menú principal de SSL**.
Generar	Genera una CSR.

Cómo ver un certificado de servidor

1. En la página **Menú principal de SSL**, seleccione **Ver certificado de servidor** y haga clic en **Siguiente**.

   La Tabla 23-5 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Haga clic en el botón correspondiente de la página **Ver certificado de servidor** para continuar.

Tabla 23-5. Información de certificados

Campo	Descripción
Número de serie	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el sujeto
Información del emisor	Atributos del certificado generados por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de vencimiento del certificado

Uso de Secure Shell (SSH)

Para obtener más información sobre SSH, consulte "Uso de Secure Shell (SSH)".

Configuración de servicios

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**. Además, la utilidad de línea de comandos de RACADM sólo se puede activar si el usuario ha iniciado sesión como **root**.

1. Amplíe el árbol de **Sistema** y haga clic en **Acceso remoto**.

2. Haga clic en la lengüeta **Configuración** y después haga clic en **Servicios**.

3. Configure los servicios siguientes según sea necesario:
   - Configuración local (Tabla 23-6)
   - Servidor web (Tabla 23-7)
   - SSH (Tabla 23-8)
   - Telnet (Tabla 23-9)
   - RACADM remota (Tabla 23-10)
   - Agente SNMP (Tabla 23-11)
   - Agente de recuperación automática del sistema (Tabla 23-12)

   Utilice el **Agente de recuperación automática del sistema** para activar la función de **Pantalla de último bloqueo** del iDRAC6.

   NOTA: Server Administrator debe estar instalado con la función **Recuperación automática** activada mediante el establecimiento de **Acción** en: **Reiniciar sistema**, **Apagar sistema** o **Realizar ciclo de encendido del sistema**, para que la opción **Pantalla de último bloqueo** funcione en el iDRAC6.

4. Haga clic en **Aplicar cambios**.

5. Para continuar, haga clic en el botón adecuado de la página **Servicios**. Vea la Tabla 23-13.

Tabla 23-6. Valores de configuración local

Valor	Descripción
Desactivar la configuración local del iDRAC por medio de la ROM de opción	Desactiva la configuración local del iDRAC por medio de la ROM de opción. La ROM de opción le pedirá que introduzca el módulo de configuración con la combinación de teclas <Ctrl+E> durante el reinicio del sistema.
Desactivar la configuración local del iDRAC por medio de RACADM	Desactiva la configuración local del iDRAC por medio de RACADM local.

Tabla 23-7. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor web. Seleccionada=activado; deseleccionada=desactivado.
Máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **Máx. de sesiones**.
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cierra cuando se alcanza la expiración de tiempo. Los cambios a la configuración del tiempo de expiración actúan de inmediato y finalizan la sesión de interfaz web actual. También se restablecerá el servidor web. Espere unos minutos antes de abrir una nueva sesión de interfaz web. El rango del tiempo de expiración es de 60 a 10800 segundos. El valor predeterminado es de 1800 segundos.
Número de puerto de HTTP	El puerto que el iDRAC utiliza para detectar una conexión de servidor. El valor predeterminado es **80**.
Número de puerto HTTPS	El puerto que el iDRAC utiliza para detectar una conexión de servidor. El valor predeterminado es **443**.

Tabla 23-8. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH Cuando está seleccionada, la casilla indica que SSH está activado.
Expiración de tiempo	La expiración de tiempo en inactividad de Secure Shell, expresado en segundos. El rango de expiración de tiempo es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de expiración de tiempo. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 23-9. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado.
Expiración de tiempo	La expiración de tiempo de inactividad del Telnet, en segundos. El rango de expiración de tiempo es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de expiración de tiempo. El valor predeterminado es **300**.
Número de	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

puerto	

Tabla 23-10. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Cuando se selecciona, la RACADM remota está activada.
Sesiones activas	El número de sesiones actuales en el sistema.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **Máx. de sesiones**.

Tabla 23-11. Configuración del agente SNMP

Valor	Descripción
Activado	Activa o desactiva el agente SNMP. Seleccionada=activado; deseleccionada=desactivado.
Nombre de comunidad	El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 23-12. Configuración del agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automática del sistema.

Tabla 23-13. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

Activación de las opciones de seguridad del iDRAC6 adicionales

Para evitar accesos no autorizados al sistema remoto, el iDRAC6 tiene las siguientes funciones:

- Filtrado de direcciones IP (IpRange): define un rango específico de direcciones IP que pueden acceder al iDRAC6.
- Bloqueo de direcciones IP: limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica

Estas funciones están desactivadas en la configuración predeterminada del iDRAC6 Utilice el subcomando siguiente o la interfaz web para activar estas funciones:

```
racadm config -g cfgRacTuning -o <nombre_de_objeto> <valor>
```

Además, use estas funciones en combinación con los valores correspondientes de expiración de tiempo de la sesión y un plan de seguridad definido para la red.

Los apartados siguientes contienen información adicional sobre estas funciones.

Filtrado de IP (IpRange)

El filtrado de direcciones IP (o *comprobación de rango IP*) permite que sólo tengan acceso al iDRAC6 los clientes o las estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Los demás inicios de sesión se rechazan.

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de **cfgRacTuning**:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propiedad **cfgRacTuneIpRangeMask** se aplica a la dirección IP entrante y a las propiedades **cfgRacTuneIpRangeAddr**. Si los resultados de ambas propiedades son idénticos, a la solicitud de inicio de sesión entrante se le concederá acceso al iDRAC6 Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión procederá si el valor de la siguiente expresión es igual a cero:

```
cfgRacTuneIpRangeMask & (<dirección_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

donde & es el operador Y a nivel de bits de las cantidades y ^ es el operador O exclusivo a nivel de bits.

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6." para ver una lista completa de las propiedades de **cfgRacTune**.

Tabla 23-14. Propiedades del filtrado de direcciones IP (IpRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación de rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Esta propiedad es una comparación con operador Y a nivel de bits con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el iDRAC6.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en forma de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior.

Activación del filtrado de IP

A continuación, se muestra un comando de ejemplo para la configuración del filtrado de IP.

Consulte "Uso de RACADM de manera remota" para obtener más información sobre RACADM y los comandos RACADM.

NOTA: Los siguientes comandos RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57.

Para restringir el inicio de sesión a una sola dirección IP (por ejemplo, 192.168.0.57), utilice toda la máscara, según se muestra a continuación.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Directrices para el filtrado de IP

Utilice las directrices a continuación cuando active el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Use la dirección base de rango que prefiera como el valor de **cfgRacTuneIpRangeAddr**. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits de orden inferior donde hay ceros en la máscara.

Bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el iDRAC6 durante un lapso de tiempo predefinido.

El parámetro de bloqueo de IP utiliza las funciones del grupo **cfgRacTuning** que incluyen:

- El número de intentos fallidos de inicio de sesión que se permiten
- El periodo en segundos dentro del que se deben presentar estos intentos fallidos
- La cantidad de tiempo en segundos que se impedirá que la dirección IP "responsable" establezca una sesión después de haber superado el número total permisible de intentos fallidos

Conforme se acumulan los intentos fallidos de inicio de sesión provenientes de una dirección IP específica, estos se "añejan" por medio de un contador interno. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: ssh exchange identification: Connection closed by remote host. (Identificación de intercambio de SSH: el host remoto cerró la conexión.)

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6" para ver una lista completa de las propiedades de **cfgRacTune**.

La Tabla 23-15 muestra una lista de los parámetros definidos por el usuario.

Tabla 23-15. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presentan intentos fallidos consecutivos (**cfgRacTuneIpBlkFailCount**) provenientes de una misma dirección IP dentro de un periodo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecer una sesión que provengan de dicha dirección se rechazarán durante un periodo establecido (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El plazo en segundos dentro del que se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.
cfgRacTuneIpBlkPenaltyTime	Define el periodo en segundos dentro del que se rechazan todos los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Activación del bloqueo de IP

El ejemplo a continuación evita que una dirección IP cliente establezca una sesión durante cinco minutos cuando el cliente ha tenido cinco intentos fallidos de inicio de sesión dentro de un periodo de un minuto.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente evita más de tres intentos fallidos dentro de un minuto y evita los intentos de inicio de sesión adicionales durante una hora.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Configuración de la seguridad de red por medio de la interfaz gráfica del usuario del iDRAC6

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC6**

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la lengüeta **Configuración** y haga clic en **Red**.
3. En la página **Configuración de red**, haga clic en **Configuración avanzada**.
4. En la página **Seguridad de la red**, configure los valores de los atributos y después haga clic en **Aplicar cambios**.

   La Tabla 23-16 describe los valores de la página **Seguridad de la red**.
5. Para continuar, haga clic en el botón adecuado de la página **Seguridad de la red**. Consulte la Tabla 23-17 para ver la descripción de los botones de la página **Seguridad de la red**.

Tabla 23-16. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de comprobación del rango de IP, que define un rango específico de direcciones IP que pueden acceder al iDRAC6.
Dirección del rango de IP	Determina el patrón de bits aceptable de la dirección IP, en función de los números 1 de la máscara de subred. Este valor es bitwise AND'd con la máscara de subred del rango IP para determinar la parte superior de una dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 pueda establecer una sesión en el iDRAC6.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior.

	Por ejemplo: **255.255.255.0**
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP.
Tiempo de penalización de bloqueo de IP	El periodo en segundos dentro del que se rechazan los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Tabla 23-17. Botones de la página de seguridad de la red

Botón	**Descripción**
Imprimir	Imprime la página **Seguridad de la red**
Actualizar	Vuelve a cargar la página **Seguridad de la red**
Aplicar cambios	Guarda los cambios que se hagan en la página **Seguridad de la red**.
Volver a la página de configuración de la red	Regresa a la página **Configuración de la red**.

Regresar a la página de contenido