Integrated Dell Remote Access Controller 6 (iDRAC6) versión 1.95

Guía del usuario

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.

03/2013

Contenido

1

Descripción general de iDRAC6

Integrated Dell Remote Access Controller6 (iDRAC6) es una solución de hardware y software de administración de sistemas que proporciona 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 del sistema 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 captura de protocolo simple de administración de red (SNMP) ante advertencias o errores. Para ayudar a diagnosticar la causa probable de un bloqueo de sistema, iDRAC6 puede registrar datos de sucesos 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 la debe configurar antes de poder 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).

Novedades de esta versión

- Compatibilidad para las configuraciones DIMM y tarjetas PCI (Para obtener más detalles consulte las Notas de la versión.)
- Compatibilidad para el explorador Internet Explorer 10.
- La longitud de la clave de cifrado de la solicitud de firma de certificado (CSR) se cambia a 2048 bits.

Funciones de administración del iDRAC6 Express

El iDRAC6 Express ofrece las siguientes funciones de administración:

- Registro de sistema dinámico de nombres de dominio (DDNS).
- Proporciona administración remota del sistema y supervisión mediante una interfaz web y la línea de comandos Server Management Command Line Protocol (SM-CLP) en una conexión serie, Telnet o SSH.
- Proporciona compatibilidad con la autentificación de Microsoft Active Directory: centraliza las identificaciones y contraseñas de usuario del iDRAC6 en Active Directory por medio del esquema estándar o del esquema extendido.
- Proporciona una solución genérica para admitir la autentificación basada en el Protocolo ligero de acceso a directorios (LDAP): esta función no requiere ninguna extensión del esquema en los servicios de directorio.
- Proporciona acceso a la información del sistema y al estado de los componentes con fines de supervisión.
- Proporciona acceso al registro de sucesos del sistema, al registro del iDRAC6, y a la pantalla de último bloqueo del sistema bloqueado o que no responde, que es independiente del estado del sistema operativo.
- Ofrece la opción de añadir notas de trabajo en el registro de Lifecycle Controller a través de la GUI o la CLI.
- Permite iniciar la interfaz web del iDRAC6 desde Dell OpenManage Server Administrator o desde Dell OpenManage IT Assistant.
- Envía alertas sobre posibles problemas del nodo administrado por medio de un mensaje de correo electrónico o una captura SNMP.
- Ofrece funciones de administración remota de la alimentación, como el apagado y el restablecimiento, desde una consola de administración.
- Ofrece compatibilidad con la Interfaz de administración de plataforma inteligente (IPMI).
- Ofrece administración remota y segura de sistemas mediante la interfaz web.
- Evita el acceso no autorizado a un sistema remoto a través de administración de seguridad de nivel de contraseña.

- Proporciona permisos asignables para distintas tareas de administración de sistemas a través de autoridad basada en funciones.
- Agrega funciones IPv6 como la capacidad de acceder a la interfaz web del iDRAC6 mediante una dirección IPv6, especifica la dirección IPv6 para el NIC del iDRAC6 y también especifica un número de destino para configurar un destino de alerta SNMP de IPv6.
- Ofrece administración accesible en la red mediante el uso del protocolo de servicios web para administración (WS-MAN).
- Agrega compatibilidad con el protocolo de línea de comandos para la administración de servidores (SM-CLP), que proporciona estándares para implementaciones de CLI de administración de sistemas.
- Permite iniciar (o revertir) a partir de la imagen de firmware seleccionada por usted a través de la reversión y recuperación de firmware.

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

iDRAC6 Enterprise y tarjeta multimedia vFlash

iDRAC6 Enterprise con tarjeta multimedios vFlash agrega compatibilidad para RACADM, la consola virtual, las funciones de medios virtuales, un NIC dedicado y vFlash (con una tarjeta multimedia Dell vFlash opcional) El uso de vFlash 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 los medios vFlash, consulte el *Manual del propietario de hardware* en **dell.com/support/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

Función	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise con vFlash
Compatibilidad con interfaces y estándares				
IPMI 2.0	✓	✓	✓	✓
Interfaz gráfica web del usuario	✗	✓	✓	✓
SNMP	✗	✓	✓	✓
WSMAN	✗	✓	✓	✓
SMASH-CLP (SSH solamente)	✗	✓	✓	✓
Línea de comandos de racadm (SSH y local)	✗	✓	✓	✓
Línea de comandos de racadm (remota)	✗	✗	✓	✓
Conectividad				
Modos de red compartida/con protección contra fallas	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
VLAN Tagging (Etiquetado VLAN)	✓	✓	✓	✓
IPv6	✗	✓	✓	✓
DNS dinámico	✗	✓	✓	✓
NIC dedicado	✗	✗	✓	✓
Seguridad y autentificación				
Autoridad basada en funciones	✓	✓	✓	✓

Tabla 1-1. Lista de funciones del iDRAC6 *(continuación)*

Función	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise con vFlash
Local Users	✓	✓	✓	✓
Cifrado SSL	✓	✓	✓	✓
Active Directory	✗	✓	✓	✓
Compatibilidad con LDAP genérico	✗	✓	✓	✓
Autentificación de dos factores[1]	✗	✓	✓	✓
Inicio de sesión único	✗	✓	✓	✓
Autentificación de PK (para SSH)	✗	✗	✓	✓
Corrección y administración remota				
Actualización remota de firmware	✓[2]	✓	✓	✓
Control de alimentación de servidor	✓[2]	✓	✓	✓
Comunicación en serie en la LAN (con proxy)	✓	✓	✓	✓
Comunicación en serie en la LAN (sin proxy)	✓	✓	✓	✓
Power Capping (Límites de alimentación)	✓	✓	✓	✓
Captura de pantalla de último bloqueo	✗	✓	✓	✓
Captura de inicio	✗	✓	✓	✓
Medios virtuales[3]	✗	✗	✓	✓

Tabla 1-1. Lista de funciones del iDRAC6 *(continuación)*

Función	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise con vFlash
Consola virtual[3]	✗	✗	✓	✓
Consola virtual compartida[3]	✗	✗	✓	✓
Inicio de la consola virtual remota	✗	✗	✓	✓
vFlash	✗	✗	✗	✓
Supervisión				
Alerta y supervisión de sensor	✓[2]	✓	✓	✓
Supervisión de alimentación en tiempo real	✓	✓	✓	✓
Gráficos de alimentación en tiempo real	✗	✓	✓	✓
Medidores de datos históricos de alimentación	✗	✓	✓	✓
Registro				
Registro de sucesos del sistema (SEL)	✓	✓	✓	✓
Registro del RAC	✗	✓	✓	✓
Registro del sistema remoto	✗	✗	✓	✓
Lifecycle Controller				
Unified Server Configurator (Configurador de servidor unificado)	✓[4]	✓	✓	✓

Tabla 1-1. Lista de funciones del iDRAC6 *(continuación)*

Función	BMC	iDRAC6 Express	iDRAC6 Enterprise	iDRAC6 Enterprise con vFlash
Servicios remotos (mediante WS-MAN)	✗	✓	✓	✓
Reemplazo de piezas	✗	✗	✗	✓

[1]La autentificación de dos factores requiere Internet Explorer.

[2]Esta función sólo está disponible mediante IPMI, y no mediante una interfaz gráfica de usuario web

[3]Consola virtual y Medios virtuales están disponibles utilizando los complementos tanto de Java como de Active-X.

[4]El Unified Server Configurator disponible mediante BMC se limita solamente a la instalación y el diagnóstico del sistema operativo.

✓ = compatible; ✗ = no compatible

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Inicio de sesión único, autentificación de dos factores y autentificación de clave pública.
- Autentificación del usuario mediante Active Directory (opcional), autentificación LDAP (opcional) o identificaciones y contraseñas de usuario almacenadas en el hardware.
- Autorización en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario.
- Configuración de identificación de usuario y contraseña por medio de la interfaz basada en web o de la CLI de SM-CLP.
- Interfaces web y SM-CLP, que son compatibles con los cifrados de 128 bits y 40 bits (para países en los que no se aceptan128 bits), usando el estándar SSL 3.0.
- Configuración de tiempo de espera de la sesión (en segundos) por medio de la interfaz web o SM-CLP.
- Puertos IP que se pueden configurar (si corresponde).

  NOTA: Telnet no admite el cifrado SSL.

- SSH, que usa una capa de transporte cifrado para ofrecer 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.
- Capacidad para limitar el rango de dirección IP para clientes que se conecten con el iDRAC6.

Plataformas admitidas

Para conocer las plataformas admitidas más recientes, consulte el archivo léame del iDRAC6 y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) disponible en **dell.com/support/manuals**.

Sistemas operativos compatibles

Para obtener la información más actualizada, consulte el archivo léame del iDRAC6 y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) disponible en **dell.com/support/manuals**.

Exploradores web admitidos

Para obtener la información más actualizada, consulte el archivo léame del iDRAC6 y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) disponible en **dell.com/support/manuals**.

NOTA: A causa de defectos serios de seguridad, se ha interrumpido la compatibilidad con SSL 2.0. Su explorador debe estar configurado para activar SSL 3.0 para que funcione correctamente. No se admite Internet Explorer 6.0.

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	• Ethernet 10 Mbps/100 Mbps • Compatibilidad con DHCP • Notificación de sucesos por correo electrónico y capturas SNMP • Compatibilidad para el shell de comandos de SM-CLP (Telnet, SSH y RACADM) 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

Port Number (Número de puerto)	Función
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Teclado/mouse de consola virtual, servicio de medios virtuales, servicio seguro de medios virtuales y vídeo de consola virtual

* Puerto configurable

Tabla 1-4. Puertos de cliente del iDRAC6

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

Otros documentos que podrían ser útiles

Además de esta guía, los siguientes documentos, disponibles en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**, proporcionan información adicional acerca de la configuración y la operación del iDRAC6 en su sistema.

- La ayuda en línea del iDRAC6 proporciona información sobre el uso de la interfaz web.
- La *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) proporciona información acerca de los subcomandos de RACADM, las interfaces admitidas, y los grupos de bases de datos de propiedades y las definiciones de objetos del iDRAC6.
- La *Guía del usuario de Dell Lifecycle Controller* proporciona información acerca de Unified Server Configurator (USC), Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE) y servicios remotos.
- Consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* para obtener información sobre el iDRAC6 y la interfaz IPMI.

- La *Matriz de compatibilidad de software de los sistemas Dell* proporciona información sobre varios de los sistemas Dell, los sistemas operativos admitidos por estos sistemas y los componentes de Dell OpenManage que pueden estar instalados en estos sistemas.
- La *Guía de instalación de Dell OpenManage Server Administrator* contiene instrucciones para ayudarlo a instalar Dell OpenManage Server Administrator.
- La *Guía de instalación de Dell OpenManage Management Station Software* contiene instrucciones para ayudarlo a instalar este software que incluye la utilidad de administración de la placa base, herramientas de DRAC y el complemento de Active Directory.
- La *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Server Administrator de Dell OpenManage) contiene información acerca de la instalación y el uso de Server Administrator.
- La *Dell Update Packages User's Guide* (Guía del usuario de Dell Update Packages) contiene información acerca de cómo obtener y utilizar los paquetes Dell Update Packages como parte de su estrategia de actualización del sistema.
- El *Glosario* proporciona información acerca de los términos utilizados en este documento.

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

- Para instalar el iDRAC6, consulte *Manual del propietario del hardware*.
- En las instrucciones de seguridad incluidas 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 **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 en bastidor* incluida con la solución de bastidor se describe cómo instalar el sistema en un bastidor.
- En la *Guía de introducción* se proporciona información general sobre las características del sistema, la configuración del sistema y las especificaciones técnicas.

- En el *Manual del propietario de hardware*, se proporciona información acerca de las funciones 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 características, 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, puesto que a menudo sustituyen la información contenida en 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.

Acceso a los documentos desde el sitio web del servicio de asistencia Dell Support

Para acceder a los documentos desde el sitio web del servicio de asistencia Dell Support:

1. Vaya a **dell.com/support/manuals**.
2. En la sección **Información sobre su sistema Dell**, en **No**, seleccione **Elegir de una lista de todos los productos Dell** y haga clic en **Continuar**.
3. En la sección **Seleccione su tipo de producto**, haga clic en **Software, supervisores, productos electrónicos y periféricos**.
4. En la sección **Elija software, supervisores, productos electrónicos y periféricos Dell**, haga clic en **Software**.

5 En la sección **Elija su software Dell**, haga clic en el vínculo requerido que corresponda:

- Client System Management
- Enterprise System Management
- Remote Enterprise System Management
- Herramientos de servicio

6 Para ver el documento, haga clic en la versión del producto requerida.

También puede acceder directamente a los documentos con los siguientes vínculos:

- Para documentos de Client System Management: **dell.com/OMConnectionsClient**
- Para documentos de Enterprise System Management: **dell.com/openmanagemanuals**
- Para documentos de Remote Enterprise System Management: **dell.com/openmanagemanuals**
- Para documentos de Herramientas de servicio: **dell.com/serviceabilitytools**

2

Introducción al iDRAC6

El iDRAC6 permite supervisar, solucionar problemas y reparar de manera remota un sistema Dell aunque el sistema esté apagado. El iDRAC6 ofrece funciones como Consola virtual, Medios virtuales, Autentificación de tarjeta inteligente e Inicio de sesión único (SSO).

La *estación de administración* es el sistema a partir del cual un administrador administra de forma remota un sistema Dell que cuenta con un iDRAC6. Los sistemas supervisados de este modo se denominan *sistemas administrados*.

De forma opcional, puede instalar el software Dell OpenManage 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 siga estos pasos generales:

NOTA: Este procedimiento puede ser distinto en diferentes sistemas. Consulte el *Manual del propietario de hardware* correspondiente a su sistema en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para obtener instrucciones específicas sobre cómo realizar este procedimiento.

1. Configure las propiedades del iDRAC6, la configuración de la red y los usuarios: el iDRAC6 se puede configurar usando la utilidad de configuración del iDRAC6, la interfaz web o RACADM.
2. **(Opcional)** Si utiliza un sistema Windows, configure Microsoft Active Directory para proporcionar acceso al iDRAC6, lo que le permite agregar y controlar privilegios de usuarios del iDRAC6 a sus usuarios existentes en el software Active Directory.
3. **(Opcional)** Configure la autentificación con tarjeta inteligente: la tarjeta inteligente proporciona un nivel adicional de seguridad a la empresa.
4. Configure los puntos de acceso remoto, como la consola virtual 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.

3

Instalación básica de un iDRAC6

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

Antes de comenzar

Compruebe que tiene los siguientes elementos incluidos con el sistema antes de instalar y configurar el software 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* (Documentación y herramientas de Dell Systems Management)

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, ver "Descripción general de la instalación y configuración del software" en la página 40.

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 un sistema para usar el iDRAC6

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

Para ejecutar la utilidad de configuración del iDRAC6:

1. Encienda o reinicie el sistema.
2. Pulse <Ctrl><E> cuando se le solicite durante la POST.

   Si el sistema operativo comienza a cargarse antes de presionar <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el sistema e inténtelo de nuevo.
3. Configure la LOM.
   a. Utilice las teclas de flecha para seleccionar los **Parámetros de LAN** y presione <Intro>. Aparece la **Selección de NIC**.
   b. Use las teclas de flecha para seleccionar uno de los siguientes modos de NIC:
      - **Dedicada**: seleccione esta opción para permitir que el dispositivo de acceso remoto utilice la interfaz dedicada de red que está disponible en el iDRAC6 Enterprise. Esta interfaz no se comparte con el sistema operativo del host y enruta el tráfico de la administración hacia una red física independiente, lo que permite separarlo del tráfico de aplicaciones. Esta opción sólo está disponible cuando el iDRAC6 Enterprise está instalado en el sistema. Después de instalar la tarjeta iDRAC6 Enterprise, asegúrese de cambiar el valor de **Selección de NIC** a **Dedicada**. Esto puede hacerse a través de la utilidad de configuración del iDRAC6, la interfaz web del iDRAC6 o RACADM.
      - **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 funciona en su totalidad cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos a través del NIC 1 y NIC 2, pero transmite datos sólo a través del NIC 1. Si el NIC 1 falla, no se podrá acceder al dispositivo de acceso remoto.

- **Compartida con LOM2 de protección contra fallas**: seleccione esta opción para compartir la interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto funciona en su totalidad cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos a través del NIC 1 y NIC 2, pero transmite datos solo a través del NIC 1. Si el NIC 1 falla, el dispositivo de acceso remoto utiliza el NIC 2 para la transmisión de todos los datos. El dispositivo de acceso remoto continúa usando el NIC 2 para la transmisión de datos. Si el NIC 2 falla, el dispositivo de acceso remoto envía todas las transmisiones de datos de regreso al NIC 1 siempre y cuando la falla en el NIC 1 se haya corregido.
- **Compartida con todas las LOM de protección contra fallas**: seleccione esta opción para compartir la interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto funciona en su totalidad cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos a través de NIC 1, NIC 2, NIC 3 y NIC 4; pero sólo transmite datos por NIC 1. Si el NIC 1 falla, el dispositivo de acceso remoto usa el NIC 2 para todas las transmisiones de datos. Si el NIC 2 falla, el dispositivo de acceso remoto usa el NIC 3 para todas las transmisiones de datos. Si el NIC 3 falla, el dispositivo de acceso remoto usa el NIC 4 para todas las transmisiones de datos. Si el NIC 4 falla, el dispositivo de acceso remoto usa el NIC 1 para todas las transmisiones de datos, sólo si la falla en la NIC 1 se ha corregido.

4 Configure los parámetros de la red de área local del controlador de red para usar DHCP o una fuente de dirección IP estática.

   a Con la tecla de flecha hacia abajo, seleccione **Parámetros de la LAN** y presione <INtro>.

   b Con las teclas de flecha hacia arriba y hacia abajo, seleccione **Fuente 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**, la **Máscara de subred** y la **Puerta de enlace predeterminada**.

e Presione <Esc>.

5 Presione <Esc>.

6 Seleccione **Guardar los cambios y salir**.

Descripción general de la instalación y configuración del software

Esta sección ofrece una descripción de alto nivel de la instalación del software iDRAC6 y del proceso de configuración. Para obtener más información acerca de los componentes del software iDRAC6, ver "Instalación del software en el sistema administrado" en la página 41.

Instalación del software iDRAC6

Para instalar el software iDRAC6:

1 Instale el software iDRAC6 en el sistema administrado. Ver "Instalación del software en el sistema administrado" en la página 41.

2 Instale el software iDRAC6 en la estación de administración. Vea la "Instalación del software en la estación de administración" en la página 42.

Configuración del iDRAC6

Para configurar el iDRAC6:

1 Use una de las siguientes herramientas de configuración:

- Interfaz web (ver "Configuración del iDRAC6 por medio de la interfaz web" en la página 49)
- Interfaz de línea de comandos de racadm (consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* [Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC] disponible en **dell.com/support/manuals**)
- Consola de Telnet (ver "Uso de una consola de Telnet" en la página 95)

NOTA: Si usa más de una herramienta de configuración del iDRAC6 al mismo tiempo, puede obtener resultados inesperados.

2 Configure los valores de red del iDRAC6. Vea la "Configuración de los valores de red del iDRAC6" en la página 118.

3 Agregue y configure usuarios del iDRAC6. Vea la "Cómo agregar y configurar usuarios del iDRAC6" en la página 139.

4 Configure el explorador web para acceder a la interfaz web. Vea la "Configuración de un explorador web admitido" en la página 46.

5 Desactive la opción de reinicio automático de Microsoft Windows. Vea la "Desactivación de la opción de reinicio automático de Windows" en la página 348.

6 Actualice el firmware del iDRAC6. Vea la "Actualización del firmware del iDRAC6" en la página 43.

Instalación del software en el sistema administrado

La instalación de software en el sistema administrado es opcional. 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 instalar el software en el sistema administrado, utilice el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management). Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida del software* disponible en el sitio web del servicio de asistencia Dell Support en **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 y el software del sistema administrado del iDRAC6 en el mismo sistema.

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

Para obtener más información sobre la pantalla de último bloqueo, ver "Visualización de la pantalla de último bloqueo del sistema" en la página 369.

Instalación del software en la estación de administración

El sistema incluye el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management). Este DVD incluye los siguientes componentes:

- Directorio raíz del DVD: contiene la utilidad Dell Systems Build and Update, que brinda 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

Para obtener información sobre Server Administrator, IT Assistant y Unified Server Configurator, consulte la *Guía del usuario de Server Administrator*, la *Guía del usuario de IT Assistant* y la *Guía del usuario de Lifecycle Controller* disponibles en el sitio web del servicio de asistencia Dell Support en **dell.com/support/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* (Documentación y herramientas de Dell Systems Management), 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* (Documentación y herramientas de Dell Systems Management) 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 obtener ayuda con el comando RACADM, escriba **racadm help** después de enviar los comandos anteriores.

Desinstalación de RACADM

Para desinstalar RACADM, abra un símbolo del sistema 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 (ver "Actualización del firmware del iDRAC6 mediante la interfaz web" en la página 44)
- Interfaz de línea de comandos de racadm (ver "Actualización del firmware del iDRAC6 mediante RACADM" en la página 44)
- Paquetes de actualización de Dell (ver "Actualización del firmware del iDRAC6 mediante paquetes de actualización de Dell para sistemas operativos Windows y Linux compatibles" en la página 45)

Antes de comenzar

Antes de actualizar el firmware del iDRAC6 con RACADM local o paquetes de actualización de Dell, 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, es posible que deba esperar hasta 30 minutos antes de que se permita otra actualización de firmware.

5. Compruebe que el USB esté activado.

Descarga del firmware del iDRAC6

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

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

- 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, ver "Actualización del firmware del iDRAC6/imagen de recuperación de los servicios del sistema" en la página 82.

Actualización del firmware del iDRAC6 mediante RACADM

Puede actualizar el firmware del iDRAC6 mediante la herramienta RACADM con 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 desde el sitio web del servicio de asistencia técnica Dell Support en **support.dell.com** al sistema administrado.

   Por ejemplo,

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

2. Ejecute el siguiente comando de RACADM:

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

   También puede actualizar el firmware usando RACADM remota 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 donde está almacenado **firmimg.d6**, incluyendo la dirección IP del servidor TFTP.

Ruta: <*IP del servidor TFTP*> -d < *Ruta de la imagen del firmware en el servidor TFTP*>

- Caso1: Si la imagen firmimg.d6 está en la carpeta raíz tftp, ruta: <*IP del servidor TFTP*>
- Caso2: Si la imagen firmimg.d6 está en la subcarpeta raíz de tftp, ruta: <*IPdelservidorTFTP*> -d /<*ruta_de_subcarpeta*>

Actualización del firmware del iDRAC6 mediante paquetes de actualización de Dell para sistemas operativos Windows y Linux compatibles

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

NOTA: Cuando se actualiza el firmware del iDRAC6 con la utilidad paquetes de actualización de Dell en Linux, pueden aparecer 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 restablecen durante el proceso de actualización del firmware pero son inofensivos.

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 en **Opciones de Internet**.
3. En la ventana **Opciones de Internet**, haga clic en la ficha **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 pide que agregue 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.

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 localizada 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 **OK** (Aceptar).
7. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.

Linux

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

1. Abra una terminal de comandos.
2. Escriba "locale" y presione <Intro>. 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 la sesión e inicie sesión en el sistema operativo.
7. Reinicie el iDRAC6.

Cuando cambie de cualquier idioma al chino simplificado, compruebe que este ajuste sigue siendo válido. De lo contrario, repita este procedimiento.

Para ver las configuraciones avanzadas del iDRAC6, ver "Configuración avanzada del iDRAC6" en la página 93.

4

Configuración del iDRAC6 por medio de la interfaz web

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, ver "Uso de la interfaz de línea de comandos SM-CLP del iDRAC6" en la página 253. Para obtener más información acerca de los comandos de RACADM, consulte la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

PRECAUCIÓN: Cuando se actualiza el navegador haciendo clic en "Actualizar" o presionando F5, es posible que la sesión en la interfaz gráfica de usuario se desconecte o que el usuario sea redirigido a la página "Resumen del sistema".

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.

   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 <Intro>.

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 <Intro>.

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

   `https://<iDRAC-IP-address>:<port-number>`

   donde *iDRAC-IP-address* es la dirección IP del iDRAC6 y *port-number* es el número del puerto HTTPS.

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

   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.

   Aparece 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 iDRAC6, 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 cuadro desplegable **Dominio**, seleccione *Este iDRAC* para iniciar sesión como usuario del iDRAC6 o seleccione cualquier dominio disponible para iniciar sesión como usuario de Active Directory.

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

Cierre de sesión

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

NOTA: El botón **Desconectar** no aparece si no se ha iniciado sesión.

NOTA: Si se cierra el explorador sin desconectarse es posible que la sesión permanezca abierta hasta agotar el tiempo de espera. Se recomienda enfáticamente hacer clic en el botón de desconexión para finalizar la sesión; de lo contrario, la sesión puede permanecer activa hasta que se agote el tiempo de espera.

NOTA: Cerrar la interfaz web del iDRAC6 en Microsoft Internet Explorer con el botón para cerrar ("x"), que se encuentra en la esquina superior derecha de la ventana, puede 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**.

PRECAUCIÓN: Si ha abierto múltiples sesiones de la interfaz web de usuario mediante <Ctrl+T> o <Ctrl+N> para acceder al mismo iDRAC6 desde una misma estación de administración y, a continuación, cierra alguna de las sesiones, todas finalizarán.

Uso de varias fichas y ventanas del explorador

Versiones diferentes de exploradores web se comportan de distinta manera al abrir nuevas fichas y ventanas. Las versiones 7 y 8 de Microsoft Internet Explorer ofrecen la opción de abrir fichas y ventanas.

Cada ficha hereda las características de la última ficha abierta.

Presione `<Ctrl-T>` para abrir una nueva ficha desde la sesión activa e iniciar sesión nuevamente.

Presione `<Ctrl-N>` para abrir una nueva ventana del explorador desde la sesión activa. Ahora está conectado con las credenciales ya autentificadas.

Al cerrar una ficha finalizan todas las fichas de interfaz Web de iDRAC6.

Además, si inicia sesión con privilegios de usuario avanzado en una ficha, y después inicia sesión como Administrador en otra ficha, ambas fichas adquieren los privilegios del primer inicio de sesión.

El comportamiento de las fichas en Mozilla Firefox 3 es igual que en las versiones 7 y 8 de Microsoft Internet Explorer.

Tabla 4-1. Comportamiento de los privilegios de usuario en exploradores admitidos

Explorador	Comportamiento de las fichas	Comportamiento de las ventanas
Microsoft Internet Explorer 6	No aplicable	Nueva sesión
Microsoft IE 7 y 8	Desde la última sesión abierta	Nueva sesión

Configuración de la NIC del iDRAC6

Esta sección supone que el iDRAC6 ya ha sido configurado y se puede tener acceso al mismo en la red. Ver "Configuración del iDRAC6" en la página 40 para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de la LAN IPMI y de red

NOTA: Para realizar los pasos siguientes, se debe tener permiso para **Configurar el iDRAC**.

NOTA: La mayoría de los servidores DHCP requiere un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este testigo 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 está usando 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 conmutador conectado al iDRAC6
- En los puertos conectados a la estación de administración que ejecutan una sesión de la consola virtual del iDRAC

NOTA: Puede aparecer el siguiente mensaje si el sistema se detiene durante la POST: `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. Una vez solucionado el inconveniente de red, reinicie el sistema.

1 Haga clic en **Configuración del iDRAC→ Red/Seguridad→ Red**.

2 En la página **Red**, puede introducir la configuración de red, la configuración común del iDRAC6 y las configuraciones de IPv4, IPv6, IPMI y VLAN. Ver Tabla 4-2, Tabla 4-3, Tabla 4-4, Tabla 4-5, la Tabla 4-6 y la Tabla 4-7 para obtener descripciones de estos valores de configuración.

3 Cuando haya introducido los valores necesarios, haga clic en **Aplicar**.

Se guardan los nuevos valores que se hayan introducido en la página Red.

NOTA: Los cambios en la configuración de la dirección IP de la NIC cierran todas las sesiones de usuario, por lo tanto, los usuarios deben volver a conectarse a la interfaz web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requieren que se restablezca la NIC, lo que provocará una breve pérdida de conectividad.

Tabla 4-2. Configuración de red

Valor	Descripción
Selección de NIC	Configura el modo actual según los cuatro modos posibles • Dedicado • Compartido (LOM1) • Compartido con LOM2 de protección contra fallas • Compartido con protección contra fallas en todas las LOM **NOTA:** La opción **Dedicada** sólo está disponible para tarjetas de iDRAC Enterprise, y la opción **Compartida con todas las LOM de protección contra fallas** podría estar disponible sólo para algunos sistemas. El iDRAC6 no se comunicará localmente mediante el mismo puerto físico si la selección de NIC está definida en modo **Compartida** o **Compartida 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. Si la selección de la NIC está definida como **Compartida con protección contra fallas** (LOM 2 o todas las LOM), se recomienda no conectar las LOM a diferentes dominios de transmisión de red. Se recomienda no agrupar las LOM con controladores de red complementarios cuando el iDRAC está configurado para cualquier modo compartido. Cualquier tipo de agrupación entre las LOM es aceptable, independientemente del modo de selección de NIC (compartida/compartida con LOM2 de protección contra fallas/compartida con todas las LOM de protección contra fallas).

Tabla 4-2. Configuración de red *(continuación)*

Valor	Descripción
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 la NIC	Cuando se selecciona, indica que la NIC está activada y activa los controles restantes en este grupo. Cuando una NIC está desactivada, toda la comunicación hacia y desde el iDRAC6 a través de la red está bloqueada. El valor predeterminado es **Activado**.
Negociación automática	Si se establece como **Activada**, muestra la velocidad de la red y el modo al comunicarse con el enrutador o conmutador más cercano. Si está **desactivada**, permite configurar la velocidad de la red y el modo dúplex de forma manual. Si **Selección de NIC** *no* está establecida en **Dedicada**, la configuración de negociación automática siempre estará **activada**. **NOTA:** Cuando el servidor está desconectado, los puertos LOM incorporados admiten una velocidad máxima de 100 Mbps. Por lo tanto, la configuración de las LOM y del conmutador para admitir la negociación automática asegura la conectividad con el iDRAC mediante transiciones de la alimentación del sistema.
Velocidad de la red	Permite configurar la velocidad de la red a 100 Mb o 10 Mb para coincidir con el 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 Semi para que coincida con el entorno de red. Esta opción no está disponible si la **negociación automática** se ha establecido como **Activada**.
MTU de NIC	Permite establecer el tamaño de la Unidad máxima de transmisión (MTU) en la NIC.

Tabla 4-3. Valores comunes

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.
Configuración automática de nombre de dominio	Utiliza el nombre del dominio DNS predeterminado. Cuando la casilla no está seleccionada y la opción **Registrar el iDRAC en DNS** está seleccionada, se puede modificar el nombre del dominio DNS en el campo **Nombre del dominio DNS**. El valor predeterminado es **Desactivado**.
Nombre de dominio de DNS	El **nombre de dominio de DNS** predeterminado está en blanco. Cuando se selecciona la casilla **Configuración automática de nombre de dominio**, esta opción se desactiva.

Tabla 4-4. Configuración de IPv4

Valor	Descripción
Activar IPv4	Si la NIC está activada, esto selecciona la compatibilidad con el protocolo IPv4 y activa los demás campos de esta sección.
Activar DHCP	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 NIC).
predeterminada	Dirección de un enrutador o un conmutador. El valor se muestra en formato de números separados con puntos, por ejemplo, 192.168.0.1.

Tabla 4-4. Configuración de IPv4 *(continuación)*

Valor	Descripción
Use DHCP para obtener direcciones del servidor DNS	Active el DHCP para obtener direcciones de servidor DNS por medio de la selección de la casilla **Usar DHCP para obtener direcciones de servidor DNS**. Cuando no se use el 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 servidor DNS** esté seleccionada, las direcciones IP no se pueden introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Dirección IP del servidor DNS.
Servidor DNS alternativo	Dirección IP del servidor DNS alternativo.

Tabla 4-5. Configuración de IPv6

Valor	Descripción
Activar IPv6	Si la casilla está seleccionada, IPv6 está activado. Si la casilla no está seleccionada, IPv6 está desactivado. El valor predeterminado es desactivado.
Activar configuración automática	Seleccione este cuadro para hacer que el iDRAC6 obtenga la dirección IPv6 para la NIC de iDRAC6 del servidor de protocolo de configuración dinámica de host (DHCPv6). Al activar la configuración automática, también se desactivan y se eliminan los valores estáticos para dirección IP 1, la longitud del prefijo y la puerta de enlace IP.
Dirección IP 1	Especifica la dirección IPv6 para la NIC del iDRAC Para cambiar esta configuración, primero debe desactivar **AutoConfig** desmarcando la casilla relacionada.
Longitud del prefijo	Configura la longitud de prefijo de la dirección IPv6. Puede tener un valor entre 1 y 128 inclusive. Para cambiar esta configuración, primero debe desactivar **AutoConfig** desmarcando la casilla relacionada.

Tabla 4-5. Configuración de IPv6 *(continuación)*

Valor	Descripción
predeterminada	Configura la puerta de enlace estática para la NIC del iDRAC. Para cambiar esta configuración, primero debe desactivar **AutoConfig** desmarcando la casilla relacionada.
Dirección local de vínculo	Especifica la dirección IPv6 local del vínculo del NIC del iDRAC6.
Dirección IP 2...15	Especifica la dirección IPv6 adicional de la NIC del iDRAC6, si hay una disponible.
Use DHCP para obtener direcciones del servidor DNS	Active el DHCP para obtener direcciones de servidor DNS por medio de la selección de la casilla **Usar DHCP para obtener direcciones de servidor 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 servidor DNS** esté seleccionada, las direcciones IP no se pueden 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 este valor, primero debe desmarcar **Usar DHCP para obtener direcciones de servidor DNS**.
Servidor DNS alternativo	Especifica la dirección IPv6 estática del servidor DNS alternativo. Para cambiar este valor, primero debe desmarcar **Usar DHCP para obtener direcciones de servidor DNS**.

Tabla 4-6. Configuración de IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando se selecciona, 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**.

Tabla 4-6. Configuración de IPMI

Valor	Descripción
Encryption Key	Configura la clave de cifrado: De 0 a 20 caracteres hexadecimales (no se permiten espacios). El valor predeterminado es todos ceros.

Tabla 4-7. Configuración de VLAN

Valor	Descripción
Activar identificación de VLAN	Si está activada, solo se acepta el tráfico con identificación de LAN virtual (VLAN) coincidente.
Id. 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.
Priority	Campo Prioridad de campos de 802.1g. Introduzca un número entre 0 y 7 para establecer la prioridad de identificación de VLAN.

Configuración de la filtración de IP y el bloqueo de IP

NOTA: Para realizar los pasos siguientes se debe tener permiso para **Configurar el iDRAC**.

1. Haga clic en **Configuración del iDRAC→ Red/seguridad** y, a continuación, en la ficha **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**.
3. Al finalizar la configuración, haga clic en **Aplicar**.

   Guarda todos los nuevos valores que se han introducido en la página Seguridad de la red.

Tabla 4-8. valores de la página de seguridad de la red

Valor	Descripción
Rango de IP activado	Activa la función de verificación del rango de IP, que define el 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 el operador Y con la máscara de subred de 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 permite establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que están fuera de este intervalo fallan. Los valores predeterminados de 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. 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 fallas de 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 fallas de bloqueo de IP	Determina el plazo en segundos durante el cual deben ocurrir el número de errores por fallos de bloque de IP para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El plazo en segundos durante el cual los intentos de inicio de sesión provenientes de una dirección IP con fallas excesivas se rechazan. El valor predeterminado es **3600**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma ofrece un mecanismo para configurar el iDRAC6 a fin de realizar las acciones seleccionadas ante ciertos mensajes de sucesos. Las acciones incluyen reiniciar el sistema, sin acción, realizar ciclo de encendido del sistema, apagar el sistema y generar una alerta (captura de sucesos de plataforma [PET] y/o correo electrónico).

Los sucesos de plataforma que se pueden filtrar se muestran en la Tabla 4-9.

Tabla 4-9. Filtros de sucesos de plataforma

Índice	Suceso de plataforma
1	Aserción de ventilador crítico
2	Aserción de advertencia de batería
3	Aserción de batería crítica
4	Aserción de voltaje crítico
5	Aserción de advertencia de temperatura
6	Aserción de temperatura crítica
7	Aserción de intromisión crítica
8	Redundancia degradada
9	Redundancia perdida
10	Aserción de advertencia de procesador
11	Aserción de procesador crítico
12	Aserción de ausencia de procesador crítica
13	Aserción de advertencia de suministro de energía
14	Aserción de suministro de energía crítico
15	Aserción de ausencia de suministro de energía crítica
16	Aserción de registro de sucesos crítico
17	Aserción de vigilancia crítica
18	Aserción de advertencia de alimentación del sistema
19	Aserción de alimentación del sistema crítica
20	Aserción informativa de medios flash extraíbles ausentes

Tabla 4-9. Filtros de sucesos de plataforma *(continuación)*

Índice	Suceso de plataforma
21	Aserción de medios flash extraíbles críticos
22	Aserción de advertencia de medios flash extraíbles

Cuando se presenta un suceso de plataforma (por ejemplo, una aserción de advertencia de la batería), se genera un suceso de sistema que se asienta en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) que está activado y se ha configurado el filtro para que genere una alerta (PET o correo electrónico), entonces se envía una alerta por correo electrónico o PET a uno o más destinos configurados.

Si el mismo filtro de sucesos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecuta.

Configuración de filtros de sucesos de plataforma (PEF)

NOTA: Configure los filtros de sucesos de plataforma antes de configurar la captura de sucesos de plataforma o las alertas por correo electrónico.

1. Inicie sesión en el sistema remoto por medio de un explorador web admitido. Ver "Acceso a la interfaz web" en la página 50.
2. Haga clic en **Sistema→ Alertas→ Sucesos de plataforma**.
3. En **Configuración de los filtros de sucesos de plataforma**, seleccione la opción **Activado** para **Activar las alertas de los filtros de sucesos de plataforma**.

   NOTA: **Permitir alertas del filtro de sucesos de plataforma** debe estar activado para que se envíe una alerta a cualquier destino válido configurado (PET o correo electrónico).

4 En la tabla **Lista de los filtros de sucesos de plataforma**, haga lo siguiente para los filtros que desee configurar:

- Seleccione una de las siguientes acciones:
  - Reiniciar sistema
  - Realizar ciclo de encendido del sistema
  - Apagar el sistema
  - Sin acción
- En la columna **Generar alerta**, seleccione la casilla de marcación para activar la generación de alertas o desmarque la casilla para desactivar la generación de alertas para la acción seleccionada.

NOTA: **Generar alerta** debe estar activado para que se envíe una alerta a cualquier destino válido configurado (PET).

5 Haga clic en **Aplicar**. La configuración se guarda.

Configuración de capturas de sucesos de plataforma (PET)

NOTA: Debe tener permiso para **Configurar el iDRAC** para agregar, activar o desactivar una alerta SNMP. Las opciones siguientes no están disponibles si no tiene permiso para **Configurar el iDRAC**.

1 Inicie sesión en el sistema remoto por medio de un explorador web admitido.

2 Asegúrese de haber realizado los procedimientos descritos en "Configuración de filtros de sucesos de plataforma (PEF)" en la página 62.

3 Haga clic en **Sistema→ Alertas→ Configuración de capturas**.

4 En la **Lista de destinos IPv4** o en la **Lista de destinos IPv6**, haga lo siguiente para el **Número de destino** para configurar el destino de las alertas SNMP de IPv4 o IPv6:

a Seleccione o deseleccione la casilla de marcación **Estado**. Una casilla de marcación seleccionada indica que la dirección IP está activada para recibir las alertas. Una casilla de marcación no seleccionada indica que la dirección IP está desactivada para la recepción de alertas.

b En **Dirección IPv4 de destino** o **Dirección IPv6 de destino**, introduzca una dirección IP de destino válida para la captura de sucesos de plataforma.

c En **Captura de prueba**, haga clic en **Enviar** para probar la alerta configurada.

NOTA: La cuenta de usuario debe tener permiso para **Probar alertas** para enviar una captura de prueba. Ver Tabla 6-6 para obtener más información.

Los cambios especificados se muestran en la **Lista de destinos** de IPv4 o IPv6.

5 En el campo **Cadena de comunidad**, introduzca el nombre de comunidad SNMP del iDRAC.

NOTA: La cadena de comunidad de destino debe ser la misma que la cadena de la comunidad del iDRAC6.

6 Haga clic en **Aplicar**. La configuración se guarda.

NOTA: Si desactiva un filtro de sucesos de plataforma, también se desactivará la captura relacionada con el sensor "defectuoso". Si la opción **Activar filtros de alerta de sucesos de plataforma** está activada, las capturas relacionadas con las transiciones de "defectuoso a buen estado" se generan siempre. Por ejemplo, si se desactiva la opción **Generar alerta** para el **Filtro de aserción informativa de medios flash extraíbles** y se quita la tarjeta SD, la captura relacionada no se muestra. La captura se genera si se vuelve a insertar la tarjeta SD. Sin embargo, si se activa la opción **Activar filtros de alerta de sucesos de plataforma**, se genera una captura cuando se quita o se inserta la tarjeta SD.

Configuración de alertas por correo electrónico

NOTA: Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio del iDRAC está configurado para que el servidor de correo reciba alertas por correo electrónico desde el iDRAC.

NOTA: Las alertas por correo electrónico admiten direcciones IPv4 e IPv6.

1 Inicie sesión en el sistema remoto por medio de un explorador web admitido.

2 Asegúrese de haber realizado los procedimientos descritos en "Configuración de filtros de sucesos de plataforma (PEF)" en la página 62.

3 Haga clic en **Sistema→ Alertas→ Configuración de las alertas por correo electrónico**.

4 En la tabla **Direcciones de correo electrónico de destino**, haga lo siguiente para configurar una dirección de destino para el **Número de alertas por correo electrónico**:

   a Seleccione o deseleccione la casilla de marcación **Estado**. Una casilla de marcación seleccionada indica que la dirección de correo electrónico está activada para recibir las alertas. Una casilla de marcación no seleccionada indica que la dirección de correo electrónico está desactivada para la recepción de mensajes de alerta.

   b En el campo **Dirección de correo electrónico de destino**, escriba una dirección válida de correo electrónico.

   c En el campo **Descripción del correo electrónico**, escriba una descripción breve.

5 En **Correo electrónico de prueba**, haga clic en **Enviar** para probar los valores de alerta de correo electrónico configurados.

6 En el campo **Dirección IP del servidor SMTP (correo electrónico)**, introduzca una dirección IP válida o FQDN (nombre de dominio completo) del servidor SMTP para que se utilice en la configuración.

   NOTA: Para enviar correctamente un correo electrónico de prueba, la **Dirección IP del servidor SMTP (correo electrónico)** debe estar configurada en la página **Configuración de las alertas por correo electrónico**. El servidor SMTP utiliza la dirección IP establecida para comunicarse con el iDRAC6 para enviar alertas por correo electrónico cuando ocurre un suceso de plataforma.

7 Haga clic en **Aplicar**. La configuración se guarda.

Configuración de IPMI por medio de la interfaz web

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 del **Sistema**, haga clic en **Configuración del iDRAC**.

   b Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Red**.

   c En la página **Red** de la **Configuración de IPMI**, seleccione **Activar IPMI en la LAN** y haga clic en **Aplicar**.

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 de IPMI 2.0.

En **Configuración de IPMI**, haga clic en el menú desplegable **Límite de nivel de privilegio del canal**, seleccione **Administrador**, **Operador** o **Usuario** y haga clic en **Aplicar**.

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 la LAN IPMI** en el campo **Clave de cifrado**, escriba la clave de cifrado y haga clic en **Aplicar**.

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 del **Sistema**, haga clic en **Configuración del iDRAC**.

b Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Comunicación en serie en la LAN**.

c En la página **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**.

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 de nivel de privilegio del canal** y seleccione **Usuario**, **Operador** o **Administrador**.

g Haga clic en **Aplicar**.

4 Configure la conexión serie de IPMI.

a En la ficha **Red/Seguridad**, haga clic en **Conexión serie**.

b En el menú **Conexión serie**, cambie el modo de la conexión serie de IPMI al valor adecuado.

En **Conexión serie de IPMI**, haga clic en el menú desplegable **Configuración 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**.

d Establezca el **Límite de nivel de privilegio del canal** y el **Control de flujo**.

e Haga clic en **Aplicar**.

f Compruebe que el multiplexor serie esté configurado correctamente en el programa de configuración del BIOS del sistema administrado.

- Reinicie el sistema.
- Durante la autoprueba de encendido, o POST, presione <F2> para entrar 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 del eco
- Edición de línea
- Nuevas secuencias de línea
- Entrada de nuevas secuencias de 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 *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guía del usuario de las utilidades de la controladora de administración de la placa base de Dell OpenManage) en **dell.com/support/manuals**.

Configuración de usuarios del iDRAC6

Para obtener más información, ver "Cómo agregar y configurar usuarios del iDRAC6" en la página 139.

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales

Esta sección ofrece información sobre las siguientes funciones de seguridad de datos 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
- Carga de un certificado de servidor
- Visualización de 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 privadas y públicas, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autentificada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Autentificarse ante un cliente habilitado con SSL
- Permitir que el cliente se autentifique 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 disponible en general 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 alta seguridad en Internet, sustituya el certificado SSL del servidor web con un certificado firmado por una autoridad de certificación reconocida. 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. Se puede entonces enviar la CSR generada a una autoridad de certificación (CA) 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 certificación (o entidad emisora de certificados) es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis confiable, identificación y otros importantes criterios de seguridad. Entre los ejemplos de autoridades de certificados se incluyen Thawte y VeriSign. Una vez que la autoridad de certificación recibe una solicitud CSR, revisa y verifica la información que contiene. 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 certificación 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.

Acceso a SSL mediante interfaz web

1. Haga clic en **Configuración del iDRAC→ Red/Seguridad**.
2. Haga clic en **SSL** para abrir la página **SSL**.

Use la página de **SSL** para realizar alguna de las opciones siguientes:

- 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.

La Tabla 4-10 describe las opciones anteriores de la página **SSL**.

Tabla 4-10. Opciones de la página SSL

Campo	Descripción
Generar solicitud de firma de certificado (CSR)	Esta opción le permite generar una CSR para enviar a una CA y solicitar un certificado de web segura. **NOTA:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. La CSR en el firmware debe coincidir con el certificado que recibió de la autoridad de certificados.
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

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 4-11 describe los atributos de la CSR.
3. Haga clic en **Generar** para crear la CSR y descargarla en su equipo local y guardarla en un directorio específico.
4. Haga clic en **Volver al menú principal de SSL** para volver a la página de SSL.

Tabla 4-11. 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, **empresaxyz.com**). Son válidos los caracteres alfanuméricos, guiones y puntos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Son válidos los caracteres alfanuméricos, guiones y puntos.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Tecnología informática). Son válidos los caracteres alfanuméricos, guiones y puntos.
Localidad	Ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Son válidos los caracteres alfanuméricos, guiones y puntos.
Nombre del estado	El estado o provincia donde se encuentra la entidad que solicita una certificación (por ejemplo, Texas). Son válidos los caracteres alfanuméricos, guiones y puntos. 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.

Carga de un certificado de servidor

1 En la página de **SSL**, seleccione **Cargar certificado del servidor** y seleccione **Siguiente**.

Aparece la página **Cargar certificado del servidor**.

2 En el campo **Ruta de acceso del archivo**, escriba la ruta de acceso del certificado del campo **Valor** o haga clic en **Examinar** para desplazarse hasta 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 **Volver al menú principal de SSL** para volver a la página del **menú principal de SSL**.

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 4-12 describe los campos y las descripciones asociadas que aparecen en la tabla **Certificado**.

2 Haga clic en **Volver al menú principal de SSL** para volver a la página del **menú principal de SSL**.

Tabla 4-12. Información de certificados

Campo	Descripción
Serial Number (Número de serie)	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el titular
Información del emisor	Atributos del certificado generados por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de vencimiento del certificado

Configuración y administración de Active Directory

La página permite configurar y administrar las configuraciones de Active Directory.

NOTA: Debe tener permiso para **Configurar el iDRAC** para usar o configurar Active Directory.

NOTA: Antes de configurar o de usar la función de Active Directory, compruebe 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 Extendido o un esquema estándar, ver "Uso del servicio de directorio del iDRAC6" en la página 155.

Para acceder a la página **Configuración y administración de Active Directory**:

1. Haga clic en **Configuración del iDRAC→ Red/Seguridad**.
2. Haga clic en **Active Directory** para abrir la página **Configuración y administración de Active Directory**.

   La Tabla 4-13 describe las opciones de la página **Configuración y administración de Active Directory**.
3. Haga clic en **Configurar Active Directory** para configurar Active Directory. Ver "Uso del iDRAC6 con Microsoft Active Directory" en la página 155 para obtener información detallada sobre la configuración.
4. Haga clic en **Probar configuración** para probar la configuración de Active Directory con la configuración especificada. Ver "Uso del iDRAC6 con Microsoft Active Directory" en la página 155 en la página 143 para obtener detalles sobre el uso de la opción Probar configuración.

Tabla 4-13. 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 autentificación de usuario de dominio, como por ejemplo nombre de usuario y contraseña. Seleccione la casilla de verificación para activar el inicio de sesión.
Selección del esquema	Especifica si se usa el esquema estándar o extendido con Active Directory. **NOTA:** En esta versión, la función de autentificación de dos factores (TFA) basada en tarjeta inteligente no se admite si Active Directory está configurado para el esquema extendido. La función de inicio de sesión único (SSO) se admite tanto para el esquema estándar como para el esquema extendido.
Nombre de dominio del usuario	Este valor contiene hasta 40 anotaciones de dominios de usuarios. Si está configurada, la lista de nombres de dominios de usuarios aparece 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.
Tiempo de espera	El tiempo de espera en segundos para que terminen las consultas a Active Directory. El valor predeterminado es 120 segundos.

Tabla 4-13. Opciones de la página Configuración y administración de Active Directory *(continuación)*

Atributo	Descripción
Buscar controladores de dominio con DNS	Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Al seleccionar esta opción, se ignoran las direcciones 1-3 del servidor del controlador de dominio. Seleccione la opción **Dominio desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** e introduzca el nombre de dominio para usar en la búsqueda en el DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema extendido**, los controladores de dominio se encuentran donde están ubicados el objeto dispositivo iDRAC6 y los objetos de asociación. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.
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. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. Si selecciona el esquema extendido, éstas son las direcciones de los controladores de dominio donde se encuentran el objeto de dispositivo del iDRAC6 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.

Tabla 4-13. Opciones de la página Configuración y administración de Active Directory *(continuación)*

Atributo	Descripción
Validación de certificados activada	El iDRAC6 usa la capa de sockets seguros (SSL) cuando se conecta a Active Directory. De manera predeterminada, el iDRAC6 utiliza el certificado de CA cargado en el iDRAC6 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 seguridad sólida. 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 certificación que firma el certificado del servidor de capa de sockets seguros (SSL) del controlador de dominio.
Configuración del esquema extendido	**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 aparecen si el iDRAC fue configurado para usar con el esquema extendido de Active Directory.

Tabla 4-13. Opciones de la página Configuración y administración de Active Directory *(continuación)*

Atributo	Descripción
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. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. 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 del grupo:** especifica el dominio del grupo. **Privilegio del grupo:** especifica el nivel de privilegios del grupo. Estos valores sólo aparecen si el iDRAC fue configurado para usar con el esquema estándar de Active Directory. Seleccione la opción **Buscar servidores de catálogo global** con DNS e introduzca el **Nombre del dominio raíz** para usarlo en una búsqueda de DNS a fin de obtener los servidores de catálogo global de Active Directory. Al seleccionar esta opción, se ignoran las **direcciones 1-3 del servidor del catálogo global**. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión satisfactoria El servidor de 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.

Configuración y administración de LDAP genérico

iDRAC6 ofrece una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP). Esta función no requiere una extensión del esquema en sus servicios de directorios. Para obtener información acerca de cómo configurar el servicio de directorio de LDAP genérico, ver "Servicio de directorio genérico de LDAP" en la página 194.

Configuración de los servicios del iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para Configurar el iDRAC.

1. Haga clic en **Configuración del iDRAC→ Red/Seguridad**. Haga clic en la ficha **Servicios** para mostrar la página de configuración **Servicios**.
2. Configure los servicios siguientes según sea necesario:
   - Configuración local: ver Tabla 4-14
   - Servidor web: ver Tabla 4-15 para consultar la configuración del servidor web.
   - SSH: ver Tabla 4-16 para consultar la configuración de SSH.
   - Telnet: ver Tabla 4-17 para consultar la configuración de Telnet.
   - RACADM remota: ver Tabla 4-18 para consultar la configuración de RACADM remota.
   - Agente SNMP: ver Tabla 4-19 para consultar la configuración de SNMP.
   - Agente de recuperación automática del sistema (ASR): ver Tabla 4-20 para consultar la configuración del agente ASR.
3. Haga clic en **Aplicar** para aplicar la configuración de la página **Servicios**.

Tabla 4-14. 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 solicita la introducción del 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 4-15. 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**.
N.º máx. de sesiones	El número máximo de sesiones del servidor web 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.
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cierra cuando se alcanza el tiempo de espera. Los cambios a la configuración del tiempo de espera actúan de inmediato y terminan la sesión de interfaz web actual. El servidor web también se restablecerá. Espere unos minutos antes de abrir una nueva sesión de interfaz web. El rango de tiempo de espera es de 60 a 10800 segundos El valor predeterminado es de 1800 segundos.

Tabla 4-15. Configuración del servidor Web *(continuación)*

Valor	Descripción
Número de puerto de 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 4-16. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando se selecciona, SSH está activado.
N.º máx. de sesiones	El número máximo de sesiones SSH simultáneas que se permite para este sistema. No se puede editar este campo. **NOTA:** El iDRAC6 admite hasta 2 sesiones SSH simultáneas.
Sesiones activas	El número de sesiones SSH actuales en el sistema, menor o igual al valor de **Máx. de sesiones**. No se puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango de tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800**.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 4-17. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, SSH está activado.
N.º máx. de sesiones	El número máximo de sesiones Telnet simultáneas que se permite para este sistema. No se puede editar este campo. **NOTA:** El iDRAC6 admite hasta 2 sesiones Telnet simultáneas.

Tabla 4-17. Configuración de Telnet

Valor	Descripción *(continuación)*
Sesiones activas	El número de sesiones Telnet actuales en el sistema, menor o igual al valor de **Máx. de sesiones**. No se puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Telnet, en segundos. El rango de tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800**.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 4-18. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Cuando se selecciona, la RACADM remota está activada.
Sesiones activas	El número actual de sesiones de RACADM remota en el sistema. No se puede editar este campo.

Tabla 4-19. Configuraciones 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. Define la cadena de comunidad de SNMP que vaya a utilizar. El nombre de comunidad puede tener hasta 31 caracteres (sin espacios). El valor predeterminado es **public**.

Tabla 4-20. Configuración del agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa/desactiva el agente de recuperación automática del sistema. Cuando se selecciona, el agente de recuperación automática del sistema está activado.

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, se puede recuperar el iDRAC6 por medio de la interfaz web del iDRAC6.

NOTA: De manera predeterminada, la actualización del firmware conserva la configuración actual del iDRAC6. Durante el proceso de actualización, tiene la opción de restablecer los valores predeterminados de fábrica para la configuración del iDRAC6. Si se establece la configuración en los valores predeterminados de fábrica, se debe configurar la red con la utilidad de configuración del iDRAC6.

1. Abra la interfaz web del iDRAC6 e inicie sesión en el sistema remoto.
2. Haga clic en **Configuración del iDRAC** y, a continuación, en la ficha **Actualizar**.
3. En la página **Cargar/Revertir (Paso 1 de 3)** haga clic en **Examinar** para seleccionar la imagen del firmware que descargó de **support.dell.com** o la imagen de recuperación de servicios del sistema.

   NOTA: Si está usando Firefox, el cursor de texto no aparece 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 carga en el iDRAC6. Este proceso puede tardar varios minutos en completarse.

   El siguiente mensaje se muestra hasta completar el proceso:

   `Carga de archivo en progreso...`

5 En la página **Estado (página 2 de 3)**, se ven los resultados de la validación realizada sobre el archivo de imagen cargada.

- Si el archivo de la imagen de recuperación del sistema se ha cargado correctamente y pasa todas las revisiones de verificación, se muestra el nombre del archivo de imagen de recuperación del sistema. Si se cargó una imagen de firmware, se muestra la versión actual de firmware y la versión nueva.

  O bien:

- Si la imagen no ha sido cargada satisfactoriamente y no aprobó todas las verificaciones, aparece un mensaje de error adecuado y la actualización regresa a la página **Cargar/Revertir (Paso 1 de 3)**. Se puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

6 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 se deselecciona la casilla de marcación **Conservar configuración**, el iDRAC6 se restablece con su configuración predeterminada. En la configuración predeterminada, la LAN está activada con una dirección IPv4 estática. No podrá iniciar sesión en la interfaz web del iDRAC6. Debe reconfigurar los valores de la LAN con la utilidad de configuración del iDRAC6 durante la POST 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 actualización de firmware, expresado en porcentaje, aparece en la columna **Progreso**.

NOTA: Mientras se encuentra en modo actualización, el proceso de actualización continua en segundo plano incluso si se aleja de esta página.

Si la actualización del firmware es satisfactoria, el iDRAC6 se restablece automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana de explorador nueva. Si se detecta un error, aparece el mensaje de error correspondiente.

Si la actualización del sistema de recuperación de servicios se completa/falla,aparece un mensaje de estado adecuado.

Reversión del firmware del iDRAC6

iDRAC6 es capaz de mantener dos imágenes de firmware simultáneamente. 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→ Configuración del iDRAC** y, a continuación, en la ficha **Actualizar**.

2. En la página **Cargar/Revertir (Paso 1 de 3)**, haga clic en **Revertir**. La versión de firmware actual y la anterior se muestran en la página **Estado (Paso 2 de 3)**.

   Conservar configuración le ofrece la opción de conservar o limpiar la configuración existente del iDRAC6. Esta opción está seleccionada de forma predeterminada.

   NOTA: Si se deselecciona la casilla de marcación **Conservar configuración**, el iDRAC6 se restablece con su configuración predeterminada. En la configuración predeterminada, la LAN está activada. Es posible que no pueda iniciar sesión en la interfaz web del iDRAC6. Debe reconfigurar los valores de la LAN con la utilidad de configuración del iDRAC6 durante la POST del BIOS o el comando racadm (disponible localmente 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 ve 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 continua en segundo plano incluso si se aleja de esta página.

   Si la actualización del firmware es satisfactoria, el iDRAC6 se restablece automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana de explorador nueva.

Registro del sistema remoto

La función de registro del sistema remoto del iDRAC6 permite escribir de manera remota el registro del RAC y el registro de sucesos del sistema (SEL) en un servidor de registro del sistema externo. Se pueden leer los registros del conjunto completo de servidores desde un registro central.

El protocolo de registro del sistema remoto no necesita ningún tipo de autentificación de usuario. Para que los registros entren al servidor de registro del sistema remoto, asegúrese de que la conectividad de red entre el iDRAC6 y el servidor de registro del sistema remoto sea correcta y de que el servidor de registro del sistema remoto se ejecute en la misma red que el iDRAC6. Las anotaciones del registro del sistema remoto son paquetes de protocolo de datagrama de usuario (UDP) que se envían al puerto de registro del sistema del servidor de registro del sistema remoto. Si se producen errores en la red, el iDRAC6 no vuelve a enviar el mismo registro. El registro remoto ocurre en tiempo real a medida que los registros ingresan al registro del RAC y al registro SEL del iDRAC6.

Es posible activar el registro del sistema remoto desde la interfaz web remota:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema**→ ficha **Configuración**→ **Configuración del registro del sistema remoto**. Aparece la pantalla **Configuración del registro del sistema remoto**.

La Tabla 4-21 indica la configuración del registro del sistema remoto.

Tabla 4-21. Configuración del registro del sistema remoto

Atributo	Descripción
Registro del sistema remoto activado	Seleccione esta opción para activar la transmisión y captura remota de registro del sistema en el servidor especificado. Una vez activado el registro del sistema, se envían nuevas anotaciones de registro a los servidores de registro del sistema.
Servidor de registro del sistema 1-3	Introduzca la dirección del servidor de registro del sistema remoto para registrar mensajes del iDRAC6 como registros SEL y del RAC. Las direcciones del servidor de registro del sistema admiten caracteres alfanuméricos y los símbolos -, ., : y _.

Tabla 4-21. Configuración del registro del sistema remoto *(continuación)*

Atributo	Descripción
Port Number (Número de puerto)	Introduzca el número de puerto del servidor de registro del sistema remoto. El número de puerto debe estar entre 1 y 65535. El predeterminado es 514.

NOTA: Los niveles de gravedad que define el protocolo de registro del sistema remoto difieren de los del registro de sucesos del sistema (SEL) de IPMI estándar. En consecuencia, todas las anotaciones de registro del sistema remoto del iDRAC6 se informan al servidor de registro del sistema con niveles de gravedad de **Aviso**.

El siguiente ejemplo muestra los objetos de configuración y el uso del comando de RACADM para cambiar la configuración de registro del sistema remoto:

```
racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogEnable [1/0]; el valor
predeterminado es 0

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer1 <nombre_del_servidor_1>;
el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer2 <nombre_del_servidor_2>;
el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogServer3 <nombre_del_servidor_3>;
el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o
cfgRhostsSyslogPort <número_de_puerto>; el valor
predeterminado es 514
```

Primer dispositivo de inicio

Esta función permite seleccionar el primer dispositivo de inicio del sistema y activa la función **Iniciar una vez**. El sistema se inicia a partir del dispositivo seleccionado en el siguiente reinicio y en los subsiguientes reinicios, y sigue siendo el primer dispositivo de inicio en el orden de inicio del BIOS mientras no sea cambiado nuevamente en la interfaz gráfica de usuario de iDRAC6 o en la secuencia de inicio del BIOS.

El primer dispositivo de inicio se puede seleccionar por medio de la interfaz web remota:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema→ Configurar→ Primer dispositivo de inicio**. Aparece la pantalla **Primer dispositivo de inicio**.

La Tabla 4-22 muestra una lista de los valores del **Primer dispositivo de inicio**.

Tabla 4-22. Primer dispositivo de inicio

Atributo	Descripción
Primer dispositivo de inicio	Seleccione el primer dispositivo de inicio en la lista desplegable. El sistema se inicia a partir del dispositivo seleccionado en el reinicio siguiente y en los inicios subsiguientes.
Iniciar una vez	Seleccionado = activado; deseleccionado = desactivado. Seleccione esta opción para iniciar a partir del dispositivo seleccionado en el siguiente inicio. En lo sucesivo, el sistema se inicia a partir del primer dispositivo de inicio en el orden de inicio del BIOS.

Recurso compartido de archivos remotos

La función Recurso compartido de archivos remotos (RFS) del iDRAC6 le permite especificar un archivo de imagen ISO o IMG ubicado en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor administrado como unidad virtual, montándolo como unidad de CD/DVD o de disco flexible mediante un sistema de archivos de red (NFS) o un sistema de archivos de Internet común (CIFS).

El formato de la ruta de acceso de la imagen compartida de CIFS es:

//<dirección IP o nombre de dominio>/<ruta de acceso a la imagen>

El formato de la ruta de acceso de la imagen compartida de NFS es:

<dirección IP>:/<ruta de acceso a la imagen>

NOTA: Si utiliza NFS, asegúrese de proporcionar la *<ruta de acceso a la imagen>* exacta, incluida la extensión del archivo de imagen, ya que distingue entre mayúsculas y minúsculas.

NOTA: <*dirección IP*> debe ser una dirección IPv4 válida. Las direcciones IPv6 no se admiten actualmente.

Si el nombre de usuario incluye un nombre de dominio, se debe introducir el nombre de usuario de la siguiente manera <*nombre de usuario*>@<*dominio*>. Por ejemplo, **user1@dell.com** es un nombre de usuario válido, mientras que **dell\user1** no lo es.

Los nombres de archivo con la extensión IMG se redireccionan como un disco flexible virtual y los nombres de archivo con la extensión ISO se redireccionan como un CDROM virtual. El recurso compartido de archivos remotos admite sólo formatos de archivo de imagen .IMG e .ISO.

La función RFS usa la implementación de medios virtuales subyacentes en el iDRAC6. Debe tener privilegios de medios virtuales para realizar un montaje de RFS. Si los medios virtuales ya utilizan una unidad virtual, la unidad no esta disponible para montarla como RFS, y viceversa. Para que RFS funcione, los medios virtuales del iDRAC6 deben estar configurados en los modos *Conectar* o *Conectar automáticamente*.

El estado de conexión del RFS se encuentra en el registro de iDRAC6. Una vez conectado, el RFS montado en la unidad virtual no se desconecta, incluso si se cierra la sesión del iDRAC6. La conexión del RFS se cierra si se restablece el iDRAC6 o se pierde la conexión a la red. Las opciones interfaz gráfica de usuario y línea de comandos también están disponibles en el iDRAC6 para cerrar la conexión del RFS.

NOTA: La función vFlash del iDRAC6 y el RFS no están relacionados.

Para activar la función Recursos compartidos de archivos remotos mediante la interfaz web del iDRAC6, haga lo siguiente:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Seleccione **Sistema**→ ficha **Recursos compartidos de archivos remotos**.

   Aparece la pantalla **Recursos compartidos de archivos remotos**.

La Tabla 4-23 indica la configuración de los recursos compartidos de archivos remotos.

Tabla 4-23. Configuración del servidor de archivos remotos

Atributo	Descripción
Nombre de usuario	Nombre de usuario para conectarse al sistema de archivos NFS/CIFS.
Contraseña	Contraseña para conectarse al sistema de archivos NFS/CIFS.
Ruta de acceso del archivo de imagen	Ruta de acceso del archivo a compartir a través de recursos compartidos de archivos remotos.
Estado	**Conectado**: el archivo se comparte. **No conectado**: el archivo no se comparte. **Conectando**: la conexión al recurso compartido está en curso.

Haga clic en **Conectar** para conectar al RFS. Después de establecer la conexión satisfactoriamente, la opción **Conectar** se desactiva.

NOTA: Incluso si ha configurado la función recursos compartidos de archivos remotos, la interfaz gráfica de usuario no muestra esta información por razones de seguridad.

Para compartir archivos de manera remota, el comando de RACADM remota es:

`racadm remoteimage`.

`racadm remoteimage <opciones>`

Las opciones son:

- `-c`: conectar imagen
- `-d`: desconectar imagen
- `-u <nombre_de_usuario>`: nombre de usuario para acceder al recurso compartido de red
- `-p <contraseña>`: contraseña para acceder al recurso compartido de red
- `-l <ubicación_de_imagen>`: ubicación de la imagen en el recurso compartido de red; indique la ubicación entre comillas
- `-s`: mostrar el estado actual

NOTA: El número máximo de caracteres admitidos parar **Nombre del usuario** y **Contraseña** es 40, y para **Ruta de acceso del archivo de imagen** es 511. Se permiten todos los caracteres para estos tres campos, incluyendo caracteres alfanuméricos y especiales, excepto los caracteres siguientes:

- ' (apóstrofe)
- " (comillas)
- , (coma)
- < (signo menor que)
- > (signo mayor que)

Módulo SD dual interno

El módulo SD dual interno (IDSDM) ofrece redundancia en la tarjeta SD del hipervisor usando otra tarjeta SD para reflejar el contenido de la primera tarjeta SD. La segunda tarjeta SD se puede configurar para IDSDM junto con la otra tarjeta SD si establece la opción **Redundancia** en **Modo de reflejo** en la pantalla **Dispositivosintegrados** de la configuración del BIOS del sistema. Para obtener más información acerca de las opciones del BIOS para IDSDM, consulte el *Manual del propietario del hardware*, disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: En la configuración del BIOS, en la pantalla **Dispositivos integrados**, la opción **Puerto USB interno** debe estar establecida en **Encendido**. Si está establecida en **Apagado**, el IDSDM no es visible par el sistema como dispositivo de inicio.

Una de las dos tarjetas SD puede ser la maestra. Por ejemplo, si se instalan dos tarjetas SD en el IDSDM mientras no hay alimentación de CA en el sistema, la SD1 se considera la tarjeta activa o maestra. La SD2 es la tarjeta de respaldo, y todas las escrituras del IDSDM del sistema de archivos irán a ambas tarjetas, pero las lecturas se realizarán solamente desde la SD1. En cualquier momento, si la SD1 falla o se extrae, la SD2 se convierte automáticamente en la tarjeta activa (maestra). La tarjeta SD vFlash está desactivada en el Modo de reflejo.

Tabla 4-24. Estado del IDSDM

IDSDM: Modo de reflejo	Tarjeta SD1	Tarjeta SD2	Tarjeta vFlash SD
Activado	Activo	Activo	Inactiva
Desactivado	Activo	Inactiva	Activo

Utilizando el iDRAC, se puede ver el estado, la condición y la disponibilidad del IDSDM.

El estado de redundancia de la tarjeta SD y los sucesos de falla se registran en SEL, se muestran en LCD, y se generan alertas PET si las alertas están activadas.

Visualización del estado del módulo de SD doble interno mediante la interfaz gráfica de usuario

1. Inicie sesión en la interfaz gráfica de usuario del iDRAC.
2. Haga clic en **Medios flash extraíbles**. Aparece la página **Medios vFlash extraíbles**. En esta página se muestran las dos secciones siguientes:

- **Módulo SD dual interno**: se muestra sólo si IDSDM está en modo redundante. El **Estado de redundancia** aparece como **Total**. Si esta sección no está presente, la tarjeta está en el estado de modo no redundante. Las indicaciones para el **Estado de redundancia** válida, son:
  - **Total**: las tarjetas SD 1 y 2 funcionan correctamente.
  - **Perdida**: una de las tarjetas SD o ambas no están funcionando correctamente.
- **Estado del módulo SD interno**: muestra el estado de la tarjeta SD para las tarjetas SD1, SD2 y vFlash, con la siguiente información:
  - Estado:
    - : indica que la tarjeta está bien.
    - : indica que la tarjeta está fuera de línea o protegida contra escritura.
    - : indica que se ha emitido una alerta.

– Ubicación: ubicación de las tarjetas SD.
– Estado en línea: las tarjetas SD1, SD2 y vFlash pueden estar en uno de los estados enumerados en la Tabla 4-25.

Tabla 4-25. Estados de las tarjetas SD

Tarjeta SD	State (Estado)	Descripción
SD1 y SD2	Boot (Inicio)	El controlador se está encendiendo.
	Activo	La tarjeta está preparada para aceptar las peticiones de lectura y escritura de la tarjeta SD.
	En espera	La tarjeta es la tarjeta secundaria. Está recibiendo una copia de todas las escrituras SD.
	Ha fallado	Se informó un error durante la lectura o escritura de una tarjeta SD.
	Ausente	La tarjeta SD no se detecta.
	Fuera de línea	Durante el inicio, la firma de identificación de la tarjeta (CID) es diferente del valor de almacenamiento no volátil (NV) o la tarjeta es el destino de una operación de copia que está en curso.
	Protegida contra escritura	La tarjeta está protegida contra escritura por el pestillo de la tarjeta SD. El IDSDM no puede utilizar una tarjeta protegida contra escritura.
vFlash	Activo	La tarjeta está preparada para aceptar las peticiones de lectura y escritura de la tarjeta SD.
	Ausente	La tarjeta SD no se detecta.

5

Configuración avanzada del iDRAC6

Esta sección ofrece información sobre la configuración avanzada del iDRAC6. Se recomienda especialmente para 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

Debe haber completado la instalación y configuración básica del hardware y software del iDRAC6. Ver "Instalación básica de un iDRAC6" en la página 37 para obtener más información.

Configuración del iDRAC6 para visualizar la salida de la conexión serie de forma remota a través de SSH/Telnet

Se puede configurar el iDRAC6 para la consola serie remota realizando los siguientes pasos:

Primero, configure el BIOS para activar la consola serie:

1. Encienda o reinicie el sistema.
2. Presione <F2> inmediatamente después de ver el siguiente mensaje:

   `<F2> = System Setup` (F2 = programa Configuración del sistema)
3. Desplácese hacia abajo y presione <Intro> para seleccionar **Comunicación serie**.
4. Configure las opciones en pantalla de la **Comunicación serie** como se indica a continuación:

   ```
   comunicación serie....Activada con
   redireccionamiento serie a través de com2
   ```

NOTA: Se puede configurar la comunicación serie en **Activada con redireccionamiento serie a través de com1** siempre que el campo de dirección del puerto serie, dispositivo serie2, también esté configurado en com1.

```
Dirección del puerto serie....Dispositivo
serie1 = com1, dispositivo serie2 = com2

conector serie externo....Dispositivo serie1

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 del sistema** y terminar la configuración del mismo.

Configuración de los valores del iDRAC6 para activar SSH/Telnet

A continuación, configure los valores del iDRAC6 para activar SSH/Telnet, lo que se puede hacer a través de RACADM o la interfaz web del iDRAC6.

Para configurar los valores del iDRAC6 para activar SSH/Telnet mediante 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 de manera remota; ver "Uso de RACADM de manera remota" en la página 120.

Para configurar los valores del iDRAC6 para activar SSH/Telnet mediante la interfaz web del iDRAC6, siga estos pasos:

1 Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.

2 Haga clic en la ficha **Red/Seguridad** y luego 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, se puede redirigir la consola de texto del sistema administrado usando **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 un símbolo del sistema 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. Se puede asignar un número menor a este valor con el comando:

```
racadm config -g cfgSerial -o cfgSerialHistorySize
<número>
```

Para configurar Linux para el direccionamiento de consola durante el inicio, ver "Configuración de Linux para la consola serie durante el inicio" en la página 99.

Uso de una consola de Telnet

Ejecución de Telnet con 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 <Intro> no responde y no aparece el indicador 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 **microsoft.com/downloads/** y busque *Windows Services for UNIX* 3.5. (Servicios de Windows para UNIX 3.5).

Activación de Telnet de Microsoft para la consola virtual Telnet

NOTA: Es posible que algunos clientes Telnet en los sistemas operativos Microsoft no muestren correctamente la pantalla de configuración del BIOS cuando la consola virtual del BIOS está configurada para la emulación de VT100/VT220. Si se presenta este problema, actualice la pantalla, cambiando la consola virtual del BIOS al modo ANSI. Para realizar este procedimiento en el menú de configuración del BIOS, seleccione **Consola virtual→ Tipo de terminal remota→ ANSI**.

NOTA: Cuando configure la ventana de emulación VT100 de cliente, configure la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas, para 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. Conecte al iDRAC6 de la estación de administración.

   Abra un símbolo del sistema, escriba lo siguiente y presione <Intro>:

   `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 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 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 usar la tecla <Retroceso>:

1. Abra una ventana de símbolo del sistema (si es necesario).
2. Si no está ejecutando ya una sesión de Telnet, escriba:

   ```
   telnet
   ```

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En el indicador, escriba:

   ```
   set bsasdel
   ```

   Aparece el mensaje siguiente:

   ```
   El retroceso se procesará como eliminación.
   ```

Para configurar una sesión de Telnet de Linux para usar la tecla <Retroceso>:

1. Abra un símbolo del sistema y escriba:

   ```
   stty erase ^h
   ```
2. En el indicador, escriba:

   ```
   telnet
   ```

Uso de Secure Shell (SSH)

Es crucial que los dispositivos del sistema y la administración de dispositivos estén protegidos. Los dispositivos incorporados y conectados son el centro medular de muchos procesos comerciales. Si estos dispositivos son vulnerables, la empresa puede estar expuesta, lo cual exige nuevas demandas de seguridad al software de administración de dispositivos de 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 autentificación por contraseña. SSH se activa en el iDRAC6 al instalar o actualizar 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 el símbolo del sistema de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

Sólo se admiten dos sesiones SSH a la vez. El fin del tiempo de espera de la sesión se controla mediante la propiedad `cfgSsnMgtSshIdleTimeout`, conforme se describe en la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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
<port number>
```

Para obtener más información acerca de las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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 del 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 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: Al configurar la ventana de emulación de cliente VT100, defina la ventana o la aplicación que está mostrando la consola virtual redirigida en 25 filas x 80 columnas, para 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 generado por anaconda
#
# Tenga en cuenta que no tiene que volver a ejecutar
grub después de hacer cambios
# en este archivo
# AVISO:  Usted no tiene una partición /boot.  Esto
significa que
#          todas las rutas de acceso de initrd o
núcleo son relativas a /, p. ej.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=
/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
predeterminado=0
tiempo de espera=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
```

Tabla 5-2. Archivo de ejemplo: /etc/grub.conf *(continuación)*

```
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**, siga las instrucciones siguientes:

1. Desactive la interfaz gráfica de GRUB y utilice la interfaz basada en texto; de lo contrario, la pantalla de GRUB no aparece en la consola virtual 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 para iniciar sesiones en la consola virtual mediante la conexión 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 virtual después del 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  Este archivo describe la manera en la que
el proceso INIT debe configurar
#          el sistema en un nivel de ejecución
determinado.
#
# Autor:  Miquel van Smoorenburg
#          Modificado para RHS Linux por Marc Ewing y
Donnie Barnes
#
# Nivel de ejecución predeterminado. Los niveles de
ejecución que utiliza RHS son:
#   0: Alto (NO establezca initdefault con este
valor)
#   1: Modo de un solo usuario
#   2: Varios usuarios, sin NFS (igual que el valor
3, si no se tiene
#       sistema en red)
#   3: Modo completo de varios usuarios
#   4: No se utiliza
#   5: X11
#   6: Reiniciar (NO establezca initdefault con este
valor)
#
id:3:initdefault:

# Inicialización del sistema.
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
```

Tabla 5-3. Archivo de ejemplo: /etc/innitab *(continuación)*

```
# Cosas que se deben ejecutar en cada nivel de
ejecución.
ud::once:/sbin/update

# Captura CTRL-ALT-SUPRIMIR
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# Cuando nuestra fuente de alimentación
ininterrumpible informe que la alimentación ha
fallado, suponer que nos quedan unos cuantos
# minutos de alimentación eléctrica restantes.
Programar un apagado en 2 minutos a partir de
este momento.
# Obviamente, esto supone que se tiene alimentación
instalada y que la
# fuente de alimentación ininterrumpible está
conectada y funciona correctamente.
pf::powerfail:/sbin/shutdown -f -h +2 "Falla de
alimentación; el sistema se está apagando"
# Si la alimentación se restaura antes de que el
apagado inicie, cancelar el apagado.
pr:12345:powerokwait:/sbin/shutdown -c "Alimentación
restaurada; se canceló el apagado"
```

Tabla 5-3. Archivo de ejemplo: /etc/innitab *(continuación)*

```
# Ejecutar gettys en los niveles de ejecución
estándares
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

# Ejecutar xdm en el nivel de ejecución 5
# xdm ahora es un servicio separado
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

NOTA: Utilice la secuencia de teclas de interrupción (~B) para ejecutar los comandos clave de Linux **Magic SysRq** en la consola serie utilizando la herramienta IPMI.

Configuración del iDRAC6 para conexión serie

Puede usar cualquiera de las interfaces siguientes para conectarse al iDRAC6 a través de una conexión serie:

- CLI de iDRAC6
- modo básico de conexión directa
- modo de terminal de conexión directa

Para configurar el sistema para usar cualquiera de estas interfaces, realice los pasos siguientes.

1. Configure el **BIOS** para activar conexiones serie:
   a. Encienda o reinicie el sistema.
   b. Presione <F2> inmediatamente después de ver el siguiente mensaje:

      `<F2> = System Setup` (F2 = programa Configuración del sistema)

   c. Desplácese hacia abajo y presione <Intro> para seleccionar **Comunicación serie**.
   d. Configure la pantalla **Comunicación serie** como se indica a continuación:

      ```
      conector serie externo....dispositivo de
      acceso remoto
      ```

   e. Seleccione **Guardar cambios**.
   f. Presione <Esc> para salir del programa **Configuración del sistema** y terminar la configuración del mismo.
2. Conecte el cable DB-9 o de módem nulo de la estación de administración al servidor de nodo administrado. Vea la "Conexión del cable de módem nulo o DB-9 para la consola serie" en la página 111.
3. Compruebe que el software de emulación de la terminal de administración esté configurado para conexiones serie. Vea la "Configuración del software de emulación de terminal de la estación de administración" en la página 111.
4. Configure los valores del iDRAC6 para activar las conexiones serie, lo que puede realizar mediante racadm o la interfaz web del iDRAC6.

Para cambiar la configuración del iDRAC6 para activar conexiones serie usando RACADM, ejecute el comando siguiente:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Para cambiar la configuración del iDRAC6 para activar conexiones serie usando la interfaz web del iDRAC6, siga estos pasos:

1. Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Conexión serie**.
3. Seleccione **Activado** en la sección **Serie de RAC**.
4. Haga clic en **Aplicar cambios**.

Si ha establecido una conexión serie con la configuración anterior, debe ver una petición de inicio de sesión. 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 sucesos 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. Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Conexión serie**.
3. Deseleccione **Activado** en la sección **Serie de RAC**.

   Para el modo básico de conexión directa:

   En la sección **Conexión serie de IPMI**, 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 **Conexión serie de IPMI**, 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, ver "Configuración de los modos conexión serie y terminal" en la página 115.

El modo básico de conexión directa permite usar herramientas como ipmish directamente a través de la conexión serie. Por ejemplo, para imprimir el registro de sucesos 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 permite 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 el inicio de sesión correcto:

```
[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 del RAC y la consola serie

El iDRAC6 admite el uso de secuencias de la tecla Esc para alternar entre la comunicación de interfaz serie del RAC y la consola serie.

Para configurar el sistema de forma tal que permita este comportamiento, siga estas instrucciones:

1 Encienda o reinicie el sistema.

2 Presione <F2> inmediatamente después de ver el siguiente mensaje:

```
<F2> = System Setup (F2 = programa Configuración
del sistema)
```

3 Desplácese hacia abajo y presione <Intro> para seleccionar **Comunicación serie**.

4 Configure la pantalla **Comunicación serie** como se indica a continuación:

comunicación serie -- Activada con redireccionamiento serie a través de com2

NOTA: Se puede configurar el campo de **comunicación serie** en **Activado con redireccionamiento a través de com1** siempre que **dispositivo serie2** en el campo de **dirección del puerto serie** también esté configurado en com1.

Dirección del puerto serie -- Dispositivo serie1 = com1, dispositivo serie2 = com2

conector serie externo -- dispositivo serie2

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 del 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 Tera Term) en la estación de administración y, de acuerdo con la etapa del proceso de inicio del servidor administrado, podrá ver las pantallas POST 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 cambiar al modo de comunicación de interfaz serie del RAC desde el modo de consola serie, utilice la siguiente secuencia de teclas:

```
<Esc> +<Mayús> <9>
```

Esta secuencia activa la petición de "Inicio de sesión del iDRAC" (si el RAC está en el modo "Serie de RAC") o bien el modo "Conexión serie" en el que pueden emitirse comandos de terminal (si el RAC se encuentra en "Modo de terminal de conexión serie directa de IPMI").

Para cambiar al modo de consola serie desde el modo de comunicación de interfaz serie del RAC, use la siguiente secuencia de teclas:

```
<Esc> +<Mayús> <q>
```

En modo de terminal, para conmutar la conexión al puerto de sistema COM2 utilice:

```
<Esc> +<Mayús> <q>
```

Al estar conectado al puerto de sistema COM2, para regresar al modo de terminal utilice:

```
<Esc> +<Mayús> <9>
```

Conexión del cable de módem nulo o DB-9 para la consola serie

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. Para que la conexión funcione con el cable de módem nulo, se deberán establecer las comunicaciones serie correspondientes 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 consola virtual de texto del 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 la misma configuración básica Utilice la información en "Valores de Minicom necesarios para la emulación de consola serie" en la página 113 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 visualiza correctamente, se recomienda que el uso de una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece la instalación de Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en el símbolo del sistema.
2. En la ventana de Xterm, lleve la flecha del mouse 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, a continuación, vaya al paso 17.
4. En el símbolo del sistema de Xterm, escriba `minicom -s`.
5. Seleccione **Configuración del puerto serie** y presione <Intro>.
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 <Intro>.
10. Seleccione **Módem y marcación** y presione <Intro>.

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 <Intro> para guardar cada uno de los valores en blanco.

13 Cuando se hayan borrado todos los campos especificados, presione <Intro> para salir del menú **Configuración de parámetros y marcación de módem**.

14 Seleccione **Guardar configuración como nombre_de_config** y presione <Intro>.

15 Seleccione **Salir de Minicom** y presione <Intro>.

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 consola virtual 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`

Compruebe que la ventana Minicom muestra un símbolo del sistema. Cuando aparezca el símbolo del sistema, 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

Tabla 5-6. Valores de Minicom para emulación de consola serie *(continuación)*

Descripción del valor	Valor necesario
Marcación de módem y configuración de parámetros	Borre los valores **init**, **reset**, **connect** y **hangup** 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 consola serie

HyperTerminal es la utilidad de acceso de puerto serie de Microsoft Windows. Para establecer el tamaño de la pantalla de la consola virtual 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 muchas funciones necesarias durante el uso de la consola virtual. Por lo tanto, utilice la edición 6.3 en su lugar o 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 consola virtual en el sistema es HyperTerminal Private de Hilgraeve.

Para configurar HyperTerminal para la 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 de 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 **OK** (Aceptar).
6. Haga clic en **Archivo→ Propiedades** y, a continuación, en la ficha **Configuración**.
7. Establezca **Identificación 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	None
Bits de parada	1
Control de flujo	Hardware

Configuración de los modos conexión serie y terminal

Configuración de la conexión serie de IPMI y del iDRAC6

1. Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Conexión serie**.
3. Configure los valores de conexión serie de IPMI.

   Ver Tabla 5-8 para consultar una descripción de los valores de conexión serie de IPMI.
4. Configure los valores de conexión serie del iDRAC6.

   Ver Tabla 5-9 para consultar una descripción de los valores de la conexión serie del iDRAC6.
5. Haga clic en **Aplicar cambios** para aplicar los cambios de la conexión serie del iDRAC6 e IPMI.
6. Haga clic en el botón correspondiente de la página **Conexión serie** para continuar. Consulte la *Ayuda en línea de iDRAC6* 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** ó **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 • User

Tabla 5-9. Configuración de la conexión serie del iDRAC6

Valor	Descripción
Activado	Activa o desactiva la consola serie del iDRAC6. Seleccionada=activada; deseleccionada=desactivada
Tiempo de espera	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 tiempo de espera.
Redirección activada	Activa o desactiva la consola virtual. 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 Esc	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 virtual. El valor máximo y predeterminado es 8192 caracteres.

Tabla 5-9. Configuración de la conexión serie del iDRAC6 *(continuación)*

Valor	Descripción
Comando de inicio de sesión	La línea de comandos del iDRAC6 que se ejecuta ante un inicio de sesión válido.

Configuración del modo de terminal

1. Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y, a continuación, en **Conexión serie**.
3. En la página **Conexión serie**, haga clic en **Configuración del modo de terminal**.
4. Defina la configuración del modo de terminal.

   Ver Tabla 5-10 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 *Ayuda en línea de iDRAC6* para ver una descripción de los botones de la página de **Configuración del modo de terminal**.

Tabla 5-10. 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 iDRAC genera un carácter <retroceso><espacio><retroceso> cuando se recibe <retroceso> o <supr>. • El iDRAC 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>.

Tabla 5-10. Configuración del modo de terminal *(continuación)*

Valor	Descripción
Introducir una nueva secuencia de línea	Seleccione <CR> o <NULL>.

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 basada en web: ver "Configuración de la NIC del iDRAC6" en la página 53.
- Interfaz de línea de comandos de RACADM: consulte cfgLanNetworking en la *RACADM iDRAC6 and CMC Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC)*, disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.
- Utilidad de configuración del iDRAC6: ver "Configuración de un sistema para usar el iDRAC6" en la página 38.

NOTA: Si se está implementando iDRAC6 en un entorno de Linux, ver "Instalación de RACADM" en la página 42.

Acceso al iDRAC6 a través de una red

Después de configurar el iDRAC6, se puede acceder de manera remota al sistema administrado por medio de una de las interfaces siguientes:

- Interfaz basada en web
- RACADM
- Consola Telnet
- SSH
- IPMI

La Tabla 5-11 describe cada interfaz del iDRAC6.

Tabla 5-11. Interfaces del iDRAC6

Interfaz	Descripción
Interfaz basada en web	Proporciona acceso remoto al iDRAC6 por medio de una interfaz gráfica de usuario. La interfaz basada en web está integrada en el firmware del iDRAC6 y se accede a ella por medio de la interfaz NIC a partir de un explorador web admitido de la estación de administración.

RACADM	Proporciona 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" en la página 120.
	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 en operaciones con 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 serie y RACADM, incluidos los comandos **powerdown**, **powerup**, **powercycle** y **hardreset**. **NOTA:** Telnet no es un protocolo seguro y transmite todos los datos, incluidas las contraseñas, en texto sin formato. Al transmitir 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 proporciona mayor seguridad.

Tabla 5-11. Interfaces del iDRAC6 *(continuación)*

Interfaz	Descripción
Interfaz IPMI	Proporciona acceso a las funciones de administración básicas del sistema remoto por medio del iDRAC6. La interfaz incluye IPMI en la LAN, IPMI en conexión serie y comunicación en serie en la LAN. Para obtener más información, consulte la *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guía del usuario de las 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 el NIC 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 de la izquierda de la página de inicio de Server Administrator, haga clic en **Sistema→ Chasis del sistema principal→ Remote Access Controller**.

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 ver una lista de los documentos relacionados, ver "Instalación básica de un iDRAC6" en la página 37.

RACADM proporciona una opción de capacidad remota (**-r**) que permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola virtual o una estación de administración remota. Para usar la capacidad remota, se 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, aparece un mensaje al escribir un comando de RACADM. Para obtener más información sobre los certificados de iDRAC6, ver "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales" en la página 68.

```
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:

```
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
```

En los sistemas Linux, asegúrese de realizar los siguientes pasos intermedios para que la validación de certificados se realice satisfactoriamente mediante racadm remota:

1. Convierta certificados en formato DER al formato PEM (mediante la herramienta openssl cmdline):

   ```
   openssl x509 -inform pem -in
   <su_cert._en_formato_der_descargado.crt> –outform
   pem -out <archivo_cert_salida_en formato_pem.pem>
   –text
   ```

2. Encuentre la ubicación del conjunto de certificados CA predeterminado en la estación de administración. Por ejemplo, para RHEL5 de 64 bits, es /etc/pki/tls/cert.pem.

3 Agregue el cerificado CA formateado como PEM al certificado CA de la estación de administración.

Por ejemplo, utilice el comando cat:

```
- cat testcacert.pem >> cert.pem
```

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 5-12 muestra una lista de las opciones del comando RACADM.

Tabla 5-12. Opciones del comando racadm

Opción	Descripción
-r <*dirección IP del RAC*>	Especifica la dirección IP?remota del controlador.
-r <*dirección IP del RAC*>:<*número de puerto*>	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.

Tabla 5-12. Opciones del comando racadm *(continuación)*

Opción	Descripción
-u <*Nombre de usuario*>	Especifica el nombre de usuario que se usa para autentificar 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 <*contraseña*>	Especifica la contraseña usada para autentificar 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 remota de RACADM se activa de manera predeterminada. Si está desactivada, 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 5-13 proporciona la descripción de cada uno de los subcomandos de RACADM que se pueden ejecutar en RACADM. Para ver una lista detallada de los subcomandos racadm, incluidas la sintaxis y las entradas válidas, consulte la *RACADM iDRAC6 and CMC Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC)* disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Al introducir un subcomando de RACADM, preceda el comando con `racadm`, por ejemplo.

```
racadm help
```

Tabla 5-13. Subcomandos de RACADM

Comando	Descripción
help	Enumera los subcomandos del iDRAC6.
help *<subcomando>*	Muestra la descripción de uso del subcomando especificado.
arp	Muestra el contenido de la tabla ARP. Las anotaciones de la tabla ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la última pantalla ASR (bloqueo) (la última pantalla azul).
clrraclog	Borra el registro del iDRAC6. Se hace una sola anotación 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 IP actual del iDRAC6.
netstat	Muestra la tabla de enrutamiento 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 enrutamiento.
setniccfg	Establece la configuración IP de la controladora.
sshpkauth	Permite cargar un máximo de 4 claves públicas SSH diferentes, eliminar claves existentes y ver las claves que ya se encuentran en el iDRAC6.
getniccfg	Muestra la configuración IP actual para la controladora.
getsvctag	Muestra las etiquetas de servicio del sistema.

Tabla 5-13. Subcomandos de RACADM *(continuación)*

Comando	Descripción
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 la alimentación en el sistema administrado.
getraclog	Muestra el registro del iDRAC6.
clrsel	Borra las anotaciones del registro de sucesos del sistema.
gettracelog	Muestra el registro de rastreo del iDRAC6. Si se usa con `-i`, el comando muestra el número de anotaciones 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	Carga una clave SSL del cliente al iDRAC6.
testtrap	Obliga al iDRAC6 a enviar una captura SNMP de prueba a través del NIC del iDRAC6 para comprobar la configuración de capturas.
vmdisconnect	Obliga el cierre de la conexión de medios virtuales.
closessn	Cierra una sesión de comunicación en el dispositivo.
getsel	Muestra las anotaciones en el Registro de sucesos del sistema (SEL).
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.
localConRedirDisable	Desactiva la consola del servidor. No hay salida del vídeo del puerto de vídeo del servidor.
testemail	Prueba la función de alertas por correo electrónico del RAC.
usercertupload	Carga un certificado de usuario o un certificado de CA de usuario del cliente en el iDRAC6.

Tabla 5-13. Subcomandos de RACADM *(continuación)*

Comando	Descripción
usercertview	Muestra el certificado de usuario o el certificado de CA de usuario que existe en el iDRAC6.
vflashsd	Inicializa u obtiene el estado de la tarjeta vFlash SD.
vflashpartition	Crea, elimina, enumera o visualiza el estado de las particiones en una tarjeta vFlash SD inicializada.

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: no se puede conectar 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 error de RACADM local: Problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de error de racadm remota: Problemas como una dirección IP, un nombre de usuario o una contraseña incorrectos.

Cuando ejecuto el comando ping en la dirección IP del iDRAC6 desde mi sistema y, a continuación, cambio el iDRAC6 entre los modos Dedicado y Compartido durante la respuesta del comando ping, no recibo respuesta.

Borre la tabla ARP en el sistema.

Racadm remota no se puede conectar al iDRAC desde SUSE Linux Enterprise Server (SLES) 11 SP1

Compruebe que ha instalado las versiones oficiales de openssl y libopenssl. Ejecute el siguiente comando para instalar los paquetes RPM:

```
rpm -ivh --force <nombre de archivo>
```

donde `<filename>` es el archivo de paquetes RPM openssl o libopenssl.

Por ejemplo,

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-
30.22.21.1.x86_64.rpm
```

Configuración de múltiples controladores iDRAC6

Por medio de RACADM, se puede configurar uno o más controladores iDRAC6 con propiedades idénticas. Al realizar una consulta en un controlador iDRAC6 específico con sus identificaciones de grupo y de objeto, RACADM crea el archivo de configuración **.cfg** a partir de la información obtenida. El usuario especifica el nombre del archivo, por ejemplo **racadm.cfg**. Si exporta el archivo a uno o varios iDRAC6, puede configurar los controladores con propiedades idénticas en poco tiempo.

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 controladores 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 un símbolo del sistema 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 el símbolo del sistema, escriba:

```
racadm config -f miarchivo.cfg
```

4 Restablezca el iDRAC6 de destino que fue configurado.

En el símbolo del sistema, escriba:

```
racadm racreset
```

El subcomando `getconfig -f racadm.cfg` solicita la configuración del iDRAC6 y genera el archivo **racadm.cfg**. Si es necesario, 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 los demás iDRAC6. Utilice **config** para sincronizar la base de datos de usuario y contraseña 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 el símbolo del sistema:

```
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. Se 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: Para obtener información acerca del comando **getconfig**, consulte el comando getconfig en la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos de iDRAC6 y CMC RACADM), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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 índice del grupo se utiliza como ancla. Todas las modificaciones a los objetos dentro del grupo indexado se asocian también con el valor del índice.

  Por ejemplo,

  ```
  [cfgUserAdmin]
  ```

```
# cfgUserAdminIndex=11

cfgUserAdminUserName=

# cfgUserAdminPassword=******** (Sólo lectura)

cfgUserAdminEnable=0

cfgUserAdminPrivilege=0x00000000

cfgUserAdminIpmiLanPrivilege=15

cfgUserAdminIpmiSerialPrivilege=15

cfgUserAdminSolEnable=0
```

- Los índices son de sólo lectura y no se pueden modificar. Los objetos del grupo indexado se vinculan al índice en el que están enumerados y todas las configuraciones válidas del valor del objeto son aplicables sólo a ese índice en particular.
- Hay un conjunto predefinido de índices disponible para cada grupo indexado. Para obtener más información, consulte la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.
- Use el subcomando **racresetcfg** para restablecer el iDRAC6 a los valores predeterminados originales y, a continuación, 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 la configuración predeterminada original y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario raíz está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas de 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 es necesario 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, a continuación, realizar un comando `racadm config -f <nombre_de_archivo>.cfg` para un iDRAC6 diferente, sin agregar caracteres de escape.

Ejemplo:

```
#

# Esto es un comentario

[cfgUserAdmin]

cfgUserAdminPageModemInitString=<Modem init # not
a comment>
```

- 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 la configuración están organizados en grupos conforme se define en la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

  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 toman 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 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.

  Para ver el contenido de un grupo indexado, use el siguiente comando:

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

  cfgUserAdminIndex=11
  ```

  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 anotaciones innecesarias de **<*variable*>=valor**. Sólo permanece la etiqueta del grupo variable real con "[" y "]", incluidas las dos anotaciones **<*variable*>=valor** que pertenecen al cambio de dirección IP.

Por ejemplo,

```
#
#   Grupo de objeto "cfgLanNetworking"
```

```
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

```
#
#   Grupo de objeto "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comentario, el resto de esta línea se ignora
cfgNicGateway=10.35.9.1
```

El comando **racadm config -f miarchivo.cfg** analiza el archivo e identifica todos los errores por número de línea. Un archivo correcto actualizará las anotaciones 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 de red disponibles, 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 activar esta función:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración del iDRAC6 al momento de inicio cuando se pide que escriba <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, ver "Configuración de un sistema para usar el iDRAC6" en la página 38.

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
MI_DOMINIO
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN del iDRAC6 se desactiva 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 protección contra fallas en todas las LOM

La Tabla 5-14 ofrece una descripción de cada modo.

Tabla 5-14. Configuraciones de NIC del iDRAC6

Modo	Descripción
Dedicado	El iDRAC6 utiliza su propio NIC (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 protección contra fallas en todas las LOM	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 indica 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 remota. 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. Al generar la solicitud de firma de certificado (CSR) que se usará para emitir el certificado, compruebe que el nombre común (CN) de la CSR coincida 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 para el nombre registrado del iDRAC**).

Para asegurarse de que la CSR coincida con el nombre DNS registrado del iDRAC6:

1. En el árbol del **Sistema**, haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y luego 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**.

Ver "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales" en la página 385 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 remota 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 la 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 configuración* > 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 solo 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 remota. 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). Ver "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales" en la página 385 para obtener más información acerca de la emisión de certificados.

6

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 obtener seguridad adicional, también puede configurar alertas que se envían por correo electrónico a usuarios específicos cuando ocurre un suceso 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 siguientes:

NOTA: Debe tener permiso para **Configurar usuarios** para poder configurar usuarios en el iDRAC.

1. Haga clic en **Configuración del iDRAC→ Red/Seguridad→ Usuarios**.

   La página **Usuarios** (ver Tabla 6-1) muestra la siguiente información para los usuarios del iDRAC6: **Identificación del usuario**, **Estado** (Activada/Desactivada), **Nombre de usuario**, **iDRAC**, **LAN**, **Puerto serie** y **Comunicación en serie en la LAN** (Activada/Desactivada).

NOTA: El usuario 1 está reservado para el usuario anónimo de IPMI y no se puede cambiar esta configuración.

2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.

En la página **Menú principal de usuarios** (ver Tabla 6-2 y Tabla 6-7), se pueden configurar usuarios, ver o cargar certificados de usuario, cargar un certificado de una autoridad de certificación (CA) de confianza, ver un certificado de CA de confianza, cargar un archivo de clave pública Secure Shell (SSH), o ver o eliminar una clave SSH específica o todas las claves SSH.

Si selecciona la opción **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página **Configuración de usuario**.

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 la **Configuración general de usuario**.
   - Los privilegios IPMI del usuario. La Tabla 6-4 describe los **Privilegios del usuario de IPMI** necesarios para configurar los privilegios de LAN del usuario.
   - 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 termine, haga clic en **Aplicar cambios**.
5. Haga clic en **Volver a la página de usuarios** para regresar a la página de usuarios.

Tabla 6-1. Estados y permisos del 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 preconfigurados. Este campo no se puede editar.
State (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.

Tabla 6-1. Estados y permisos del usuario *(continuación)*

Valor	Descripción
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 exclusivo. **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.
iDRAC	Muestra el grupo (nivel de privilegio) al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
LAN	Muestra el nivel de privilegio de LAN de IPMI al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
Serial Port (Puerto serie)	Muestra el nivel de privilegio del puerto serie de IPMI al que está asignado el usuario (Administrador, Operador, Sólo lectura o Ninguno).
Serial Over LAN (Comunicación en serie en la LAN)	Permite o revoca el permiso del usuario para usar la comunicación en serie en la LAN de IPMI.

Tabla 6-2. Opciones de configuración de la tarjeta inteligente

Opción	Descripción
Cargar certificado de usuario	Permite que el usuario cargue el certificado de usuario al iDRAC6 y que lo importe al perfil del usuario.
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 usuario

Opción	Descripción
Identificación de usuario	Uno de los 16 números de identificación de usuario predefinidos.
Activar el usuario	Cuando está seleccionado, indica que el acceso del usuario al iDRAC6 está activado. Cuando no está seleccionado, el acceso del usuario está desactivado.
Nombre de usuario	Un nombre de usuario de hasta 16 caracteres. Se admiten los siguientes caracteres: • 0-9 • A-Z • A-Z • Caracteres especiales: + %) ' > : $ [| ! & = * , - { § # (? < ; _ } I
Cambiar contraseña	Activa los campos **Contraseña nueva** y **Confirmar nueva contraseña**. Si se borran, la Contraseña del usuario no se puede cambiar.
Contraseña nueva	Introduzca una **Contraseña** de hasta 16 caracteres. Los caracteres no se muestran y aparecen enmascarados. Se admiten los siguientes caracteres: • 0-9 • A-Z • A-Z • Caracteres especiales: + & ? > - } | . ! (' , _ [" @ #) * ; $ / § % = < : { I \
Confirmar contraseña nueva	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 la 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 como uno de los siguientes: **Administrador**, **Operador**, **Sólo lectura** o **Ninguno**. Ver Tabla 6-6 para ver los **Permisos de grupo del iDRAC**.
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Permite al usuario otorgar permisos de acceso al sistema a usuarios específicos. **PRECAUCIÓN: Este privilegio se reserva normalmente para los usuarios que son miembros de la función de Administrador en el iDRAC. Sin embargo, este privilegio se les puede asignar a los usuarios con la función "Operador". Un usuario con este privilegio puede modificar la configuración de cualquier usuario. Esto incluye la creación o eliminación de cualquier usuario, la administración de la clave SSH para usuarios, etc. Por estos motivos, asigne este privilegio con cuidado.**
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.

Tabla 6-5. Privilegios del usuario del iDRAC *(continuación)*

Propiedad	Descripción
Acceder a la consola virtual	Permite al usuario ejecutar la consola virtual.
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 otorgados
Administrador	Iniciar sesión en el iDRAC, Configurar el iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
Operador	Selecciona cualquier combinación de los siguientes permisos: Iniciar sesión en el iDRAC, Configurar el iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de acción del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
Sólo lectura	Inicio de sesión en iDRAC
Ninguno	Sin permisos asignados

Autentificación de la clave pública en el SSH

El iDRAC6 admite la autentificación de clave pública (PKA) a través de SSH. Este método de autentificación mejora la automatización de secuencias de comandos de SSH al eliminar la necesidad de incorporar o solicitar la identificación/contraseña del usuario.

Antes de comenzar

Puede configurar hasta 4 claves públicas *por usuario* que pueden ser utilizadas en la interfaz de SSH. Antes de agregar o eliminar claves públicas, no deje de utilizar el comando view para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente una de ellas. Si la autentificación de claves públicas (PKA) en la SSH se define y usa correctamente, no tendrá que introducir el nombre de usuario ni la contraseña al iniciar sesión en el iDRAC6. Esto puede ser muy útil para configurar secuencias de comandos automatizadas para realizar distintas funciones.

Cuando se prepare para configurar esta función, tenga en cuenta lo siguiente:

- Puede administrar está función con RACADM y también con la GUI.
- Al agregar claves públicas nuevas, verifique que las claves existentes no se encuentren ya en el índice donde se agregará la clave nueva. iDRAC6 no realiza comprobaciones para verificar que las claves anteriores se han eliminado antes de agregar una nueva. Tan pronto se agrega una clave nueva, automáticamente entra en vigor siempre que la interfaz de SSH esté activada.

Generación de claves públicas para Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que accederá al iDRAC6 en la SSH. Hay dos maneras de generar el par de claves públicas/privadas: Usando la aplicación *Generador de claves PuTTY* para clientes que ejecutan Windows o la interfaz de línea de comandos *ssh-keygen* para clientes que ejecutan Linux. La utilidad *ssh-keygen* de CLI está incluida de forma predeterminada en todas las instalaciones estándar.

Esta sección describe instrucciones sencillas para generar un par de claves públicas/privadas en ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la ayuda de la aplicación.

Para usar el *generador de claves PuTTY* para los clientes de Windows y crear la clave básica:

1. Inicie la aplicación y seleccione SSH-2 RSA o SSH-2 DSA para el tipo de clave a generar. (SSH-1 no está admitido).
2. Los algoritmos admitidos para generar claves son RSA y DSA únicamente. Introduzca el número de bits para la clave. El número debe estar entre 768 y 4096 bits para RSA y 1024 bits para DSA.
3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica. Después de crear la clave, se puede modificar el campo de comentario de la clave. También se puede introducir una frase contraseña para asegurar la clave. Verifique que ha guardado la clave privada.
4. Puede guardar la clave pública en un archivo con la opción "Guardar clave pública" para cargarla posteriormente. Todas las claves cargadas deben estar en formato RFC 4716 u openssh. De lo contrario, deberá convertir la misma a dicho formato.

Generación de claves públicas para Linux

La aplicación *ssh-keygen* para clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario.

Abra una ventana de terminal y en el indicador de shell introduzca:

```
ssh-keygen -t rsa -b 1024 -C testing
```

NOTA: Las opciones distinguen entre mayúsculas y minúsculas.

donde,

la opción **-t** puede ser *dsa* o *rsa*.

la opción **–b** especifica el tamaño de cifrado de bits entre 768 y 4096.

la opción **–C** permite modificar el comentario de clave pública y es opcional.

Siga las instrucciones. Después de que el comando se ejecute, cargue el archivo público.

PRECAUCIÓN: Las claves generadas desde la estación de administración Linux con ssh-keygen no tienen el formato 4716. Convierta las claves al formato 4716 con el comando `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. **No cambie los permisos del archivo de clave. La conversión anterior deberá realizarse con los permisos predeterminados.**

NOTA: iDRAC6 no admite el envío ssh-agent de claves.

Inicio de sesión con autentificación de clave pública

Después de cargar las claves públicas, se puede iniciar sesión en el iDRAC6 mediante SSH sin introducir una contraseña. También tendrá la opción de enviar un solo comando de RACADM como argumento de línea de comandos a la aplicación de SSH. Las opciones de línea de comandos se comportan como RACADM remota, pues la sesión finaliza al completarse el comando.

Por ejemplo,

Conectar:

```
nombre de usuario ssh@<dominio>
```

o

```
nombre de usuario ssh@<dirección_IP>
```

donde dirección_IP es la dirección IP del iDRAC6.

Envío de comandos racadm:

```
nombre de usuario ssh@<dominio> racadm getversion
nombre de usuario ssh@<dominio> racadm getsel
```

Carga, visualización y eliminación de claves SSH mediante la interfaz web del iDRAC6

1. Haga clic en **Configuración del iDRAC→ Red/Seguridad→ Usuarios**. Aparece la página **Usuarios**.
2. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario. Aparece la página **Menú principal de usuarios**.
3. Use las opciones de **Configuraciones de claves SSH** para cargar, ver o eliminar claves SSH.

PRECAUCIÓN: La capacidad de cargar, ver y/o eliminar claves SSH depende del privilegio de usuario "Configurar usuarios". Este privilegio les permite a los usuarios configurar la clave SSH de otro usuario. Se debe tener cuidado al otorgar este privilegio. Para obtener más información sobre los privilegios de usuarios, ver "Cómo agregar y configurar usuarios del iDRAC6" en la página 139.

Tabla 6-7. Configuraciones de claves SSH

Opción	Descripción
Cargar claves SSH	Permite al usuario local cargar un archivo de clave pública Secure Shell (SSH). Si se carga una clave, el contenido del archivo de la clave aparece en un cuadro de texto no editable, en la página **Configuración del usuario**.
Ver/eliminar claves SSH	Permite al usuario local ver o eliminar una clave SSH especificada o todas las claves SSH.

La página **Cargar claves SSH** permite cargar un archivo de clave pública Secure Shell (SSH). Si se carga una clave, el contenido del archivo de clave aparece en un cuadro de texto no editable en la página **Ver/eliminar claves SSH**.

Tabla 6-8. Cargar claves SSH

Opción	Descripción
Archivo o texto	Seleccione la opción **Archivo** y escriba la ruta de acceso donde se encuentra la clave. También puede seleccionar la opción **Texto** y copiar el contenido del archivo de la clave en el cuadro. Puede cargar nuevas claves o sobrescribir las existentes. Para cargar un archivo de clave, haga clic en **Explorar**, seleccione el archivo y haga clic en el botón **Aplicar**.
Examinar	Haga clic en este botón para ubicar la ruta de acceso completa y el nombre del archivo de la clave.

La página **Ver o quitar clave(s) SSH** le permite ver o quitar las claves públicas SSH del usuario.

Tabla 6-9. Ver/eliminar claves SSH

Opción	Descripción
Remove (Quitar)	En el cuadro aparece la clave cargada. Seleccione la opción Eliminar y haga clic en **Aplicar** para eliminar la clave existente.

Carga, visualización y eliminación de claves SSH usando RACADM

Cargar

El modo de carga permite cargar un archivo de clave o copiar el texto de la clave en la línea de comandos. No es posible cargar y copiar una clave al mismo tiempo.

RACADM local y RACADM remota

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -f
<nombre_de_archivo>

racadm sshpkauth -i <2 a 16> -k <1 a 4> -t

<texto-de-la-clave>
```

RACADM Telnet/SSH/serie:

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -t

<texto-de-la-clave>
```

Ejemplo:

Cargue una clave válida para el usuario 2 del iDRAC6 en el espacio de la primera clave con un archivo:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

El archivo de clave de autentificación PK SSH se cargó correctamente en el RAC.

PRECAUCIÓN: La opción "texto de la clave" se admite en la racadm remota y local. La opción "archivo" no se admite en la RACADM Telnet/SSH/serie.

Ver

El modo de visualización le permite al usuario ver una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -v -k <1 a 4>

racadm sshpkauth -i <2 a 16> -v -k all
```

Eliminar

El modo de eliminación le permite al usuario eliminar una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -d -k <1 a 4>

racadm sshpkauth -i <2 a 16> -d -k all
```

Para obtener información acerca de las opciones de subcomando, consulte el subcomando `sshpkauth` en la *iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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 de esta sección como guía para crear un archivo de proceso por lotes de comandos RACADM y después ejecute el archivo de proceso por lotes en cada sistema administrado.
- Cree el archivo de configuración del iDRAC6 conforme se describe en la *iDRAC6 and CMC Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC)* disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** y ejecute el subcomando **racadm config** en cada sistema administrado utilizando el 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, ya que 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 con el tiempo. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC6.

Para verificar si el usuario existe, escriba el comando siguiente en el símbolo del sistema:

```
racadm getconfig -u <nombre_de_usuario>
```

O bien:

escriba el siguiente comando una vez para cada índice de 1 a 16:

```
racadm getconfig -g cfgUserAdmin -i <index>
```

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 se activa o desactiva manualmente un usuario con el subcomando **racadm config**, se *debe* especificar el índice con la opción **-i**. Observe 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 usuario nuevo 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:
   - iDRAC
   - LAN
   - Serial Port (Puerto serie)
   - Serial Over LAN (Comunicación en serie en la 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 john

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 siguientes comandos:

```
racadm getconfig -u juan

racadm getconfig –g cfgUserAdmin –i 2
```

Eliminación de un usuario del iDRAC6

Cuando se usa RACADM, los usuarios se deben desactivar manual e individualmente. Los usuarios no se pueden eliminar por medio de un archivo de configuración.

El siguiente ejemplo muestra la sintaxis del comando que se puede usar para eliminar un usuario del iDRAC6:

```
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 la configuración del usuario en los valores predeterminados originales de fábrica.

Activación de un usuario del iDRAC6 con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones), primero localice un índice de usuario disponible mediante los pasos descritos en "Antes de comenzar" en la página 150. A continuación, escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña:

NOTA: Para ver una lista de valores válidos de máscara de bits para privilegios de usuario específicos, consulte la *iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support, en **dell.com/support/manuals**. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios activados.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <índice> <valor de máscara de
bits de privilegio del usuario>
```

7

Uso del servicio de directorio del iDRAC6

Un servicio de directorio mantiene una base de datos común para almacenar información sobre los usuarios, equipos, impresoras, etc. de una red. Si la empresa utiliza el software Microsoft Active Directory o el software de servicio de directorio de LDAP, puede configurarlo para que proporcione acceso al iDRAC6, lo que permite agregar y controlar los privilegios de usuarios del iDRAC6 para los usuarios existentes del servicio de directorio.

Uso del iDRAC6 con Microsoft 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.

Puede configurar la autentificación de usuario mediante Microsoft Active Directory para iniciar sesión en el iDRAC6. También puede proporcionar autoridad basada en la función, lo que activa al administrador para configurar privilegios específicos para cada usuario. Para obtener más información, consulte las secciones subsiguientes.

La Tabla 7-1 muestra los 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.

Tabla 7-1. Privilegios de usuario del iDRAC6 *(continuación)*

Privilegio	Descripción
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a la consola virtual	Permite al usuario ejecutar la consola virtual.
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.

Se puede utilizar Active Directory para iniciar sesión en el iDRAC6 mediante uno de los siguientes métodos:

- Interfaz basada en web
- RACADM remoto
- Consola serie o Telnet

La sintaxis de inicio de sesión es la misma para los tres métodos:

<nombre_de_usuario@dominio>

o

*<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 enumera todos los dominios de usuario en el menú desplegable para que elija. Si selecciona un dominio de usuario del menú desplegable, sólo debe introducir el nombre de usuario. Si selecciona **Este iDRAC**, podrá iniciar sesión como usuario de Active Directory si utiliza la sintaxis de inicio de sesión descrita anteriormente en esta sección.

También puede iniciar sesión en el iDRAC6 mediante tarjeta inteligente o con el inicio de sesión único. Para obtener más información, consulte "Configuración del iDRAC6 para inicio de sesión único o inicio de sesión mediante tarjeta inteligente" en la página 205.

NOTA: El servidor de Windows 2008 Active Directory admite sólo una cadena de <*nombre_de usuario*>@<*nombre_de_dominio*> con un máximo de 256 caracteres.

Prerrequisitos para activar la autentificación de Microsoft Active Directory para iDRAC6

Para usar la función de autentificación 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 autentificar 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 autentificar 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. Ver "Activación de SSL en un controlador de dominio" en la página 158 para obtener información más específica.

Activación de SSL en un controlador de dominio

Cuando el iDRAC autentifica 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 también se carga en el iDRAC. En otras palabras, para que el iDRAC pueda autentificarse en *cualquier* controlador de dominio —sin importar si es el controlador de dominio raíz o secundario— el controlador de dominio debe tener un certificado activado con SSL firmado por la CA del dominio.

Si va a usar la CA 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:

Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.

1. Haga clic en **Inicio→ Herramientas administrativas→ Política de seguridad del dominio**.
2. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
3. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
4. Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado raíz de CA del controlador de dominio al iDRAC6

NOTA: Si el sistema ejecuta Windows 2000 o si está utilizando una CA independiente, los siguientes pasos pueden variar.

1. Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **Start** (Inicio)→ **Run** (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 **Terminar**.

9 Haga clic en **OK** (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 en él con el botón derecho del mouse, 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 paso 14 en el iDRAC.

Para cargar el certificado mediante RACADM, ver "Configuración de Microsoft Active Directory con esquema extendido con la interfaz web del iDRAC6" en la página 176 o "Configuración de Microsoft Active Directory con esquema estándar mediante RACADM" en la página 189.

Para cargar el certificado mediante la interfaz de web, ver "Configuración de Microsoft Active Directory con esquema extendido con la interfaz web del iDRAC6" en la página 176 o "Configuración de Microsoft Active Directory con esquema estándar mediante la interfaz web del iDRAC6" en la página 185.

Importación del certificado SSL de firmware del iDRAC6

NOTA: Si el servidor de Active Directory está configurado para autentificar el cliente durante una fase de inicialización de sesión SSL, se debe cargar también el certificado de servidor del iDRAC6 en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autentificación 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 certificados de raíz confiables del controlador de dominio, no es necesario realizar los pasos detallados en esta sección.

El certificado SSL del iDRAC6 es el certificado idéntico que se usa para el servidor web del iDRAC6. Todos los controladores del iDRAC se envían con un certificado predeterminado firmado automáticamente.

Para descargar el certificado SSL del iDRAC6, ejecute el siguiente comando de 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 mouse 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 iDRAC6 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 el certificado esté en la lista **Autoridades de certificación de raíz confiables**. 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 **Terminar** y luego en **Aceptar**.

Mecanismos de autentificación compatibles de Active Directory

Se puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: la solución de *esquema extendido*, que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell.

También se puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las siguientes secciones 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 extendido o de esquema estándar.

Las ventajas de usar la solución de esquema extendido 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 extensión del esquema, ya que la configuración predeterminada del esquema de Active Directory de Microsoft proporciona todas las clases de objetos necesarias.

Generalidades del esquema ampliado de Active Directory

Para utilizar la solución de esquema extendido, es necesario una extensión del esquema de Active Directory, según se describe en la siguiente sección.

Extensiones de esquema 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 extender la base de datos de Active Directory al agregar sus propios atributos y clases exclusivos para solucionar las necesidades específicas del entorno. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory debe ser definido con una identificación única. Para que las identificaciones se mantengan exclusivas en toda la industria, Microsoft conserva una base de datos de Identificadores de Objeto de Active Directory (OID) para que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán exclusivas y no entrarán en conflicto una con otra. Para extender 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.

Extensión de Dell: dell

OID base de Dell: 1.2.840.113556.1.8000.1280

Rango de LinkID del RAC: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 extendido 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 iDRAC. Este modelo ofrece máxima flexibilidad al Administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC y dispositivos iDRAC en la red sin aumentar demasiado la complejidad.

Descripción general de los objetos de Active Directory

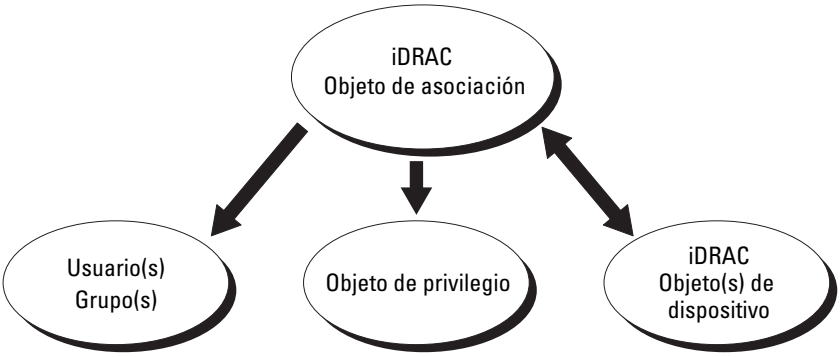
Para cada uno de los iDRAC físicos en la red que desee integrar con Active Directory para autentificación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de iDRAC. Puede crear varios objetos de asociación, y cada objeto de asociación puede vincularse a cuantos usuarios, 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 iDRAC) a un solo 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 autentificación 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 autentificación 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 autentificar.

La Ilustración 7-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autentificaciones y autorizaciones.

Ilustración 7-1. Configuración típica de los objetos de Active Directory



Se pueden crear tantos objetos de asociación como sean necesarios. Sin embargo, debe crearse al menos un objeto de asociación y debe tener un objeto de dispositivo iDRAC por cada iDRAC de la red que desea integrar con Active Directory para autentificación y autorización con iDRAC.

El objeto de asociación permite toda cantidad de usuarios o grupos, así como de objetos de dispositivo iDRAC. Sin embargo, el objeto de asociación solo 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 producto del objeto de asociación.

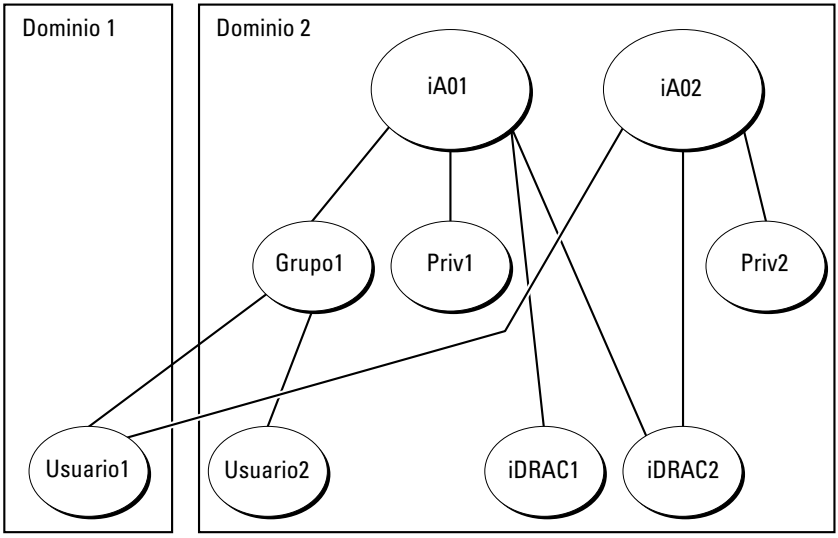
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema extendido admiten todo tipo de grupos de usuarios o de grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autentificación del esquema extendido admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados al mismo usuario entre distintos objetos de asociación. En otras palabras, la autentificación del esquema extendido 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 Ilustración 7-2 muestra un ejemplo de la acumulación de privilegios por medio del esquema extendido.

Ilustración 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; mientras que 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 autentificación del esquema extendido 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 con esquema extendido para acceder al iDRAC6

Antes de usar Active Directory para acceder al iDRAC6, configure el software Active Directory y el iDRAC6 llevando a cabo los pasos siguientes:

1. Amplíe el esquema de Active Directory (ver "Cómo extender el esquema de Active Directory" en la página 166).
2. Amplíe el complemento Usuarios y equipos de Active Directory (ver "Instalación de la extensión de Dell para el complemento Usuarios y equipos de Microsoft Active Directory" en la página 173).
3. Agregue usuarios del iDRAC6 y sus privilegios a Active Directory (ver "Cómo agregar usuarios y privilegios del iDRAC a Microsoft Active Directory" en la página 174).

4 Configure las propiedades de Active Directory del iDRAC6 mediante la interfaz web del iDRAC6 o RACADM (ver "Configuración de Microsoft Active Directory con esquema extendido con la interfaz web del iDRAC6" en la página 176 o "Configuración de Microsoft Active Directory con esquema extendido mediante RACADM" en la página 179).

Cómo extender el esquema de Active Directory

Importante: la extensión del esquema de este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Se debe extender el nuevo esquema e instalar el nuevo complemento Microsoft Management Console (MMC) de usuarios y equipos de Active Directory en el directorio. El esquema anterior no funciona con este producto.

NOTA: El extender el nuevo esquema y la instalación de la nueva extensión en el complemento de usuarios y equipos de Active Directory no afecta los productos anteriores.

El complemento MMC de Usuarios y equipos de Active Directory y la extensión del esquema se encuentran en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management). Para obtener información sobre la instalación, ver "Instalación de la extensión de Dell para el complemento Usuarios y equipos de Microsoft Active Directory" en la página 173. Para obtener detalles adicionales acerca de la extensión del esquema para iDRAC6 y la instalación del complemento MMC de Usuarios y equipos de Active Directory, consulte la *Dell OpenManage Installation and Security User's Guide* (Guía del usuario de instalación y seguridad de Dell OpenManage), disponible en **dell.com/support/manuals**.

NOTA: Al crear objetos de asociación o de dispositivo iDRAC, asegúrese de seleccionar **Dell Remote Management Object Advanced**.

La extensión del esquema de Active Directory agrega una unidad organizacional Dell, clases y atributos de esquema, así como privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender 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 extender el esquema por medio de uno de los siguientes métodos:

- 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* (Documentación y herramientas de Dell Systems Management) en los siguientes directorios respectivamente:

- *Unidad de DVD*:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <*Unidad* de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender

NOTA: La carpeta **Remote_Management** sirve para extender el esquema con productos de acceso remoto anteriores, como DRAC 4 y DRAC 5, puesto que la carpeta **Remote_Management_Advanced** sirve para extender el esquema en el iDRAC6.

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**. Para usar Dell Schema Extender para extender el esquema de Active Directory, ver "Uso de Dell Schema Extender" en la página 167.

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 **Terminar**.

El esquema ha sido extendido. Para verificar la extensión del esquema, utilice el complemento de esquema de Active Directory y MMC y verifique si existen los siguientes elementos:

- Clases (ver Tabla 7-2 a 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 a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
Superclases	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
Superclases	almacenamiento
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
Superclases	None
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
Superclases	User
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
Superclases	Computadora
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 distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este atributo es el vínculo para avanzar al vínculo dellAssociationMembers. Identificación de vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO

Tabla 7-8. Lista de atributos agregados al esquema de Active Directory *(continuación)*

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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)	VERDADERO
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)	VERDADERO
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)	VERDADERO
delIsLogClearAdmin 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)	VERDADERO
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)	VERDADERO
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de consola virtual 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)	VERDADERO
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)	VERDADERO

Tabla 7-8. Lista de atributos agregados al esquema de Active Directory *(continuación)*

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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)	VERDADERO
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)	VERDADERO
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)	VERDADERO
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)	VERDADERO
dellAssociationMembers Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO

Instalación de la extensión de Dell para el complemento Usuarios y equipos de Microsoft Active Directory

Cuando se extiende el esquema en Active Directory, también debe extenderse el complemento 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.

Al instalar el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) se puede instalar el complemento seleccionando la opción **Complemento Usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la *Dell OpenManage Software Quick Installation Guide* (Guía de instalación rápida del software Dell OpenManage) para obtener más instrucciones sobre la instalación del software Systems Management. Para sistemas operativos Windows de 64 bits, el instalador del complemento se ubica en **<DVD drive>:\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 de Administrator Pack

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, ver "Cómo abrir el complemento de usuarios y equipos de Microsoft Active Directory" en la página 173.

Cómo abrir el complemento de usuarios y equipos de Microsoft Active Directory

Para abrir el complemento de usuarios y equipos de Active Directory:

1. Si está conectado en la controladora del dominio, haga clic en **Inicio→ Herramientas administrativas→ Usuarios y equipos de Active Directory**.

   Si no está conectado en la controladora de dominio, debe tener el Microsoft Administrator Pack correspondiente instalado en el sistema local. Para instalar este paquete de administrador, haga clic en **Inicio→ Ejecutar**, escriba `MMC` y presione **Intro**.

   Aparece 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 **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar**.

5 Haga clic en **Cerrar** y luego en **Aceptar**.

Cómo agregar usuarios y privilegios del iDRAC a Microsoft Active Directory

El complemento Usuarios y equipos de Active Directory que Dell ha extendido permite agregar usuarios y privilegios del iDRAC mediante la creación de objetos de asociación y de privilegio del iDRAC. Para agregar cada tipo de objeto, realice los pasos siguientes:

- Cree un objeto de dispositivo iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Configuración de un objeto de asociación

Creación de un objeto de dispositivo iDRAC

1 En la ventana **Raíz de consola** de MMC, haga clic con el botón derecho del mouse en un contenedor.

2 Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

Se abre la ventana **Nuevo objeto**.

3 Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC que va a escribir en el Paso A de "Configuración de Microsoft Active Directory con esquema extendido con la interfaz web del iDRAC6" en la página 176.

4 Seleccione **Objeto de dispositivo de iDRAC**.

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

Cómo crear 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 consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Se abre la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **OK** (Aceptar).
6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
7. Haga clic en la ficha **Privilegios de administración remota** y seleccione los privilegios que desea otorgar al usuario.

Cómo crear 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 consola** (MMC), haga clic con el botón derecho del mouse 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. Haga clic en **OK** (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 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 mouse en **Objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre del usuario o grupo de usuarios y haga clic en **Aceptar**.

Haga clic en la ficha **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 autentifican en un dispositivo iDRAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

1. Seleccione la ficha **Objetos de privilegios** y haga clic en **Agregar**.
2. Escriba el nombre del objeto de privilegio y haga clic en **Aceptar**.

Haga clic en la ficha **Productos** para agregar un dispositivo iDRAC conectado a la red disponible para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos iDRAC a un objeto de asociación.

Cómo agregar dispositivos iDRAC

Para agregar dispositivos iDRAC:

1. Seleccione la ficha **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 Microsoft Active Directory con esquema extendido 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. Vaya a **Configuración del iDRAC**→ ficha **Red/Seguridad**→ ficha **Servicio de directorio**→ **Microsoft Active Directory**.
4. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparece la página **Paso 1 de 4** de **Configuración y administración de Active Directory**.

5 En **Configuración de certificados**, seleccione **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9.

6 En **Cargar 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.

7 Haga clic en **Cargar**.

Aparece la información del certificado de CA de Active Directory que se cargó.

8 **(Opcional: para autentificación AD)** En **Cargar archivo keytab de Kerberos**, 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 carga en el iDRAC6.

9 Haga clic en **Siguiente**. Aparece la página **Paso 2 de 4** de **Configuración y administración de Active Directory**.

10 Seleccione la opción **Habilitar Active Directory**.

PRECAUCIÓN: En esta versión, la función de autenticación de dos factores (TFA) con tarjeta inteligente no puede utilizarse si Active Directory está configurado para el esquema extendido. La función de inicio de sesión único (SSO) se admite tanto para el esquema estándar como para el esquema extendido.

11 Haga clic en **Agregar** para introducir el nombre de dominio de usuario.

12 Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**.

NOTA: 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. Se puede elegir de la lista y luego sólo escribir el nombre de usuario.

13 En el campo **Tiempo de espera**, escriba el tiempo (en segundos) que el iDRAC debe esperar para obtener las respuestas de Active Directory. El valor predeterminado es 120 segundos.

14 Seleccione una de las opciones siguientes:

a **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory a partir de una búsqueda en el DNS. Se ignoran las direcciones 1 a 3 del servidor del controlador de dominio. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. O bien, seleccione **Especificar un dominio** e introduzca el nombre del dominio que se usará en la búsqueda de DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema extendido**, los controladores de dominio se encuentran donde está el objeto de dispositivo del iDRAC6 y los objetos de asociación.

b Seleccione la opción **Especificar direcciones de controlador de dominio** para permitir que el iDRAC6 utilice las direcciones de servidor del controlador de dominio de Active Directory que se especifican. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Cuando se selecciona la opción **Especificar direcciones del controlador de dominio**, se debe configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. Si selecciona el **esquema extendido**, éstas son las direcciones de los controladores de dominio donde se encuentran el objeto de dispositivo del iDRAC6 y los objetos de asociación.

NOTA: El nombre de dominio completo o la dirección IP que se especifique en el campo **Dirección del servidor de controlador de dominio** debe coincidir con el campo Asunto o Nombre alternativo del asunto del certificado del controlador de dominio, si se tiene activada la validación de certificados.

15 Haga clic en **Siguiente**. Aparece la página **Paso 3 de 4** de **Configuración y administración de Active Directory**.

16 En **Selección del esquema**, haga clic en **Esquema extendido**.

17 Haga clic en **Siguiente**. Aparece la página **Paso 4 de 4** de **Configuración y administración de Active Directory**.

18 En **Configuración del esquema extendido**, escriba el **Nombre del iDRAC** y el **Nombre de dominio del iDRAC** para configurar el objeto de dispositivo iDRAC. El nombre de dominio del iDRAC es el dominio en el que se crea el objeto del iDRAC.

19 Haga clic en **Finalizar** para guardar la configuración del esquema extendido de Active Directory.

El servidor web del iDRAC6 automáticamente regresa a la página **Configuración y administración de Active Directory**.

20 Haga clic en **Probar configuración** para controlar la configuración del esquema extendido de Active Directory.

21 Escriba su nombre de usuario y contraseña de Active Directory.

Aparecen los resultados de la prueba y el registro de la misma. Para obtener información adicional, ver "Prueba de las configuraciones realizadas" en la página 193.

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Haga clic en la página **Configuración del iDRAC→ Red/seguridad→ Red** para configurar los servidores DNS manualmente o para usar DHCP para obtener los servidores DNS.

Con este paso se completa la configuración de Active Directory con esquema extendido.

Configuración de Microsoft Active Directory con esquema extendido mediante RACADM

Use los comandos siguientes para configurar el componente Microsoft Active Directory del iDRAC6 con el esquema extendido mediante la herramienta de CLI de RACADM, en lugar de la interfaz web.

1 Abra un símbolo del sistema 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 del RAC>

racadm config -g cfgActiveDirectory -o
cfgADRacDomain <nombre completo del dominio del RAC>

racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <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, una a la vez, hasta lograr establecer una conexión satisfactoria. Cuando selecciona la opción de esquema extendido, estas 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 extendido.

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, la función de autenticación de dos factores (TFA) con tarjeta inteligente no puede utilizarse si Active Directory está configurado para el esquema extendido. La función de inicio de sesión único (SSO) se admite tanto para el esquema estándar como para el esquema extendido.

Si desea utilizar la búsqueda en el DNS para obtener la dirección del servidor del controlador de dominio de Active Directory, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- Para realizar la búsqueda en el DNS con el nombre de dominio del usuario que inicia sesión:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- Para especificar el nombre de dominio que se utilizará en la búsqueda en el DNS:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <nombre de dominio
  que se utilizará en la búsqueda en el DNS>
  ```

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 entidad emisora.

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 la entidad emisora con el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

```
racadm sslcertupload -t 0x2 -f <certificado CA raíz
de ADS>
```

El siguiente comando de RACADM es opcional. Consulte “Importación del certificado SSL de firmware del iDRAC6” en la página 159 para obtener información adicional.

```
racadm sslcertdownload -t 0x1 -f <certificado raíz
SSL de RAC>
```

2 Si desea especificar el tiempo en segundos que se debe esperar a que las consultas de Active Directory (AD) se completen antes de que finalice el tiempo de espera, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <tiempo en segundos>
```

3 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
```

4 Si el DHCP está desactivado 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>
```

5 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.

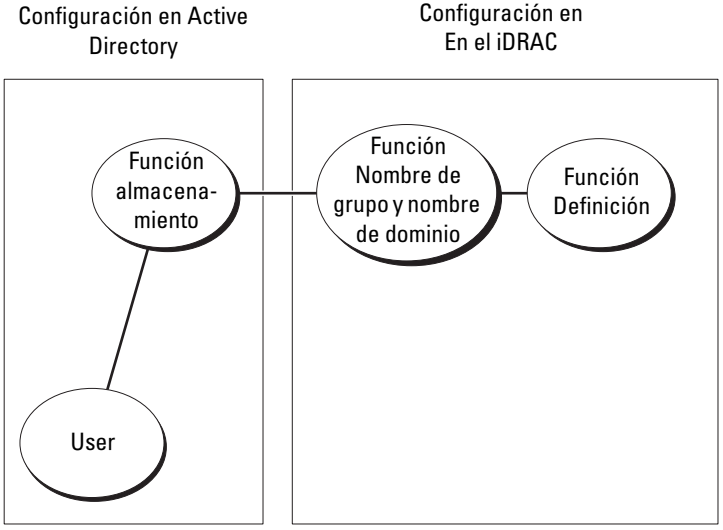
Ver "Servicio de directorio genérico de LDAP" en la página 194 para obtener información detallada sobre los dominios de usuario.

6 Presione **Intro** para completar la configuración de Active Directory con esquema extendido.

Generalidades del esquema estándar de Active Directory

Como se muestra en Ilustración 7-3, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en iDRAC6.

Ilustración 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 extendido, 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.

NOTA: El nivel de privilegio del grupo de funciones predeterminado para los cinco grupos de funciones es **Ninguno**. Debe escoger uno de los privilegios predeterminados del grupo de funciones desde la casilla desplegable.

Tabla 7-9. Privilegios predeterminados del grupo de funciones

Nivel de privilegio	Permisos otorgados	Máscara de bits
Administrador	Iniciar sesión en el iDRAC, Configurar el iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000001ff
Operador	Iniciar sesión en el iDRAC, Configurar el iDRAC, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000000f9
Sólo lectura	Inicio de sesión en iDRAC	0x00000001
Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan solamente cuando se establece el esquema estándar utilizando RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios que inician sesión y los grupos de funciones, así como los grupos anidados, están en el mismo dominio, en el iDRAC6 sólo se deben configurar las direcciones de los controladores de dominio. En este caso de dominio único, se admiten todos los tipos de grupos.

Si todos los usuarios que inician sesión y los grupos de funciones, o cualquiera de los grupos anidados, pertenecen a múltiples dominios, en el iDRAC6 se deben configurar las direcciones del servidor de catálogo global. En este caso de dominios múltiples, todos los grupos de funciones y los grupos anidados, si los hay, deben ser del tipo Grupo universal.

Configuración de Active Directory con esquema estándar para acceder al iDRAC6

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. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al iDRAC6.
3. Configure el nombre del grupo y el nombre del dominio en el iDRAC6 mediante la interfaz web o RACADM. Para obtener más información, consulte "Configuración de Microsoft Active Directory con esquema estándar mediante la interfaz web del iDRAC6" en la página 185 o "Configuración de Microsoft Active Directory con esquema estándar mediante RACADM" en la página 189.

Configuración de Microsoft Active Directory con esquema estándar mediante la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Vaya a **Configuración del iDRAC**→ ficha **Red/Seguridad**→ ficha **Servicio de directorio**→ **Microsoft Active Directory**.
4. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparece la página **Paso 1 de 4** de **Configuración y administración de Active Directory**.
5. En **Configuración de certificados**, seleccione **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9.
6. En **Cargar certificado de CA de Active Directory**, explore el equipo para encontrar el archivo del certificado.
7. Haga clic en **Cargar**.

   Aparece la información del certificado de CA de Active Directory válido.

8 **(Opcional: para autentificación AD)** En **Cargar archivo keytab de Kerberos**, 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 carga en el iDRAC6.

9 Haga clic en **Siguiente**. Aparece la página **Paso 2 de 4** de **Configuración y administración de Active Directory**.

10 Seleccione la opción **Habilitar Active Directory**.

11 Seleccione la opción **Activar inicio de sesión único** si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autentificación de usuario de dominio, como por ejemplo un nombre de usuario y contraseña.

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**.

14 En el campo **Tiempo de espera**, escriba el tiempo (en segundos) que el iDRAC debe esperar para obtener las respuestas de Active Directory. El valor predeterminado es 120 segundos.

15 Seleccione una de las opciones siguientes:

a **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory a partir de una búsqueda en el DNS. Se ignoran las direcciones 1 a 3 del servidor del controlador de dominio. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. O bien, seleccione **Especificar un dominio** e introduzca el nombre del dominio que se usará en la búsqueda de DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.

b Seleccione la opción **Especificar direcciones del controlador de dominio** para permitir que el iDRAC6 utilice las direcciones del servidor del controlador de dominio de Active Directory que se especifican. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Cuando se selecciona la opción **Especificar direcciones del controlador de dominio**, se debe configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. En el **esquema estándar**, estas son las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

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**. Aparece la página **Paso 3 de 4** de **Configuración y administración de Active Directory**.

17 En **Selección del esquema**, seleccione **Esquema estándar**.

18 Haga clic en **Siguiente**. Aparece la página **Paso 2 de 4** de **Configuración y administración de Active Directory**.

19 Seleccione una de las opciones siguientes:

- Seleccione la opción **Buscar servidores de catálogo global con DNS** e introduzca el **Nombre del dominio raíz** para usarlo en una búsqueda de DNS a fin de obtener los servidores de catálogo global de Active Directory. Se ignoran las direcciones 1 a 3 del servidor de catálogo global. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión satisfactoria El servidor de 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.

- Seleccione la opción **Especificar direcciones del servidor de catálogo global** e introduzca la dirección IP o el nombre de dominio completo (FQDN) de los servidores de catálogo global. La búsqueda en el DNS no se realizó. Al menos una de las tres direcciones debe estar configurada. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. El servidor de 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.

NOTA: El nombre de dominio completo o la dirección IP que se especifique en el campo **Dirección del servidor de catálogo global** debe coincidir con el campo Sujeto o Nombre alternativo del sujeto del certificado del controlador de dominio, si se 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.

20 En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

Aparece la página **Paso 4b de 4** de Configuración y administración de Active Directory.

21 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.

22 Especifique el **Dominio del grupo de funciones**, que es el dominio del grupo de funciones.

23 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 ese nivel de permiso.

24 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.

25 Si es necesario, configure más grupos de funciones.

26 Haga clic en **Finalizar** para regresar a la página **Configuración y administración de Active Directory**.

27 Haga clic en **Probar configuración** para controlar la configuración del esquema estándar de Active Directory.

28 Escriba su nombre de usuario y contraseña de iDRAC6.

Aparecen los resultados de la prueba y el registro de la misma. Para obtener información adicional, ver "Prueba de las configuraciones realizadas" en la página 193.

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Haga clic en la página **Configuración del iDRAC→ Red/seguridad→ Red** para configurar los servidores DNS manualmente o para usar DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema estándar.

Configuración de Microsoft Active Directory con esquema estándar mediante RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC con esquema estándar con la interfaz de línea de comandos de RACADM, en lugar de hacerlo con la interfaz web.

1 Abra un símbolo del sistema 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 ver los valores de Número de máscara de bits, consulte la *RACADM iDRAC6 and CMC Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio del servicio de asistencia Dell Support, en **dell.com/support/manuals**.

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <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, una por una, hasta lograr una conexión satisfactoria. 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.

Si desea utilizar la búsqueda en el DNS para obtener la dirección del servidor del controlador de dominio de Active Directory, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable 1
```

- Para realizar la búsqueda en el DNS con el nombre de dominio del usuario que inicia sesión:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain 1
  ```

- Para especificar el nombre de dominio que se utilizará en la búsqueda en el DNS:

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <nombre de dominio
  que se utilizará en la búsqueda en el DNS>
  ```

Para especificar la dirección del servidor de Catálogo global, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog1 <nombre de dominio completo o dirección
IP del controlador de dominio>
```

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog2 <nombre de dominio completo o dirección
IP del controlador de dominio>
```

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
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 utilizar la búsqueda en el DNS para obtener la dirección del servidor de Catálogo global de Active Directory, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o
cfgADGcSRVLookupEnable 1
```

```
racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain <Nombre de dominio>
```

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 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 CA raíz
de ADS>
```

El siguiente comando de RACADM es opcional. Consulte "Importación del certificado SSL de firmware del iDRAC6" en la página 159 para obtener información adicional.

```
racadm sslcertdownload -t 0x1 -f <certificado raíz
SSL de RAC>
```

2 Si desea especificar el tiempo en segundos que se debe esperar a que las consultas de Active Directory (AD) se completen antes de que finalice el tiempo de espera, escriba el siguiente comando:

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <tiempo en segundos>
```

3 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
```

4 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>
```

5 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 <índice>
```

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40. Ver "Servicio de directorio genérico de LDAP" en la página 194 para obtener información acerca de dominios de usuario.

Prueba de las configuraciones realizadas

Si desea verificar si la configuración funciona o si desea diagnosticar el problema en caso de errores al iniciar sesión en Active Directory, puede realizar pruebas de 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. Aparece 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, examine 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 comunes, ver "Preguntas frecuentes acerca de Active Directory" en la página 200.

Si desea efectuar cambios en la configuración, haga clic en la ficha **Active Directory** y modifique la configuración según las instrucciones detalladas.

Servicio de directorio genérico de LDAP

iDRAC6 ofrece una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP). Esta función no requiere una extensión del esquema en sus servicios de directorios.

Para realizar la implementación genérica de LDAP del iDRAC6, se usa la característica común entre distintos servicios de directorio para agrupar a los usuarios y luego asignar la relación del grupo de usuarios. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener distintos nombres de atributo para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se pueden configurar en iDRAC6.

Sintaxis de inicio de sesión (usuario de directorio y usuario local)

A diferencia de Active Directory, no se utilizan caracteres especiales ("@", "\", y "/") para diferenciar un usuario LDAP de un usuario local. El usuario de inicio de sesión sólo debe introducir el nombre de usuario, y omitir el nombre de dominio. iDRAC6 toma el nombre de usuario tal cual se indica y no lo desglosa en nombre de usuario y dominio del usuario. Cuando se activa el LDAP genérico, iDRAC6 primero intenta conectar al usuario como usuario de directorio. Si esto falla, se activa la búsqueda de usuario local.

NOTA: No hay modificación de comportamiento en la sintaxis de inicio de sesión de Active Directory. Cuando el LDAP genérico está activado, la página de la interfaz gráfica de usuario para inicio de sesión sólo muestra "Este iDRAC" en el menú desplegable.

NOTA: Los caracteres "<" y ">" no se permiten en el nombre de usuario para los servicios de directorio basados en openLDAP y OpenDS.

Configuración del servicio de directorio LDAP genérico mediante la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.

3 Vaya a **Configuración del iDRAC**→ ficha **Red/Seguridad**→ ficha **Servicio de directorio**→ **Servicio de directorio de LDAP genérico**.

La página **Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico de iDRAC6. Desplácese hasta el final de la página **Configuración y administración de LDAP genérico** y haga clic en **Configurar LDAP genérico**.

Aparece la página Paso 1 de 3 de **Configuración y administración de LDAP genérico**. Use esta página para configurar el certificado digital que se utiliza durante el inicio de las conexiones de SSL al comunicarse con un servidor LDAP genérico. Estas comunicaciones usan el LDAP a través de SSL (LDAPS). Si activa la convalidación de certificados, cargue el certificado de la Autoridad de certificados (CA) que emitió el certificado utilizado por el servidor LDAP durante el inicio de las conexiones de SSL. El certificado de CA se usa para convalidar la autenticidad del certificado proporcionado por el servidor LDAP durante el inicio de SSL.

NOTA: En esta versión, no se admite el enlace al LDAP basado en puertos distintos a SSL. Sólo se admite el LDAP a través de SSL.

4 En **Configuración del certificado**, seleccione **Activar validación del certificado** para activar la validación del certificado. Si esta opción está activada, iDRAC6 utiliza el certificado de CA para validar el certificado del servidor LDAP durante el enlace del nivel de conexión segura (SSL); si está desactivada, iDRAC6 omite el paso de validación de certificados del enlace de SSL. Es posible desactivar la validación de certificados durante las pruebas o si el administrador del sistema decide confiar en los controladores de dominio en el límite de seguridad sin validar sus certificados de SSL.

PRECAUCIÓN: Asegúrese de que la opción CN = abrir LDAP FQDN esté configurada (por ejemplo: CN = openldap.lab) en el campo de asunto del certificado del servidor LDAP, durante la generación del certificado. El campo de dirección del servidor LDAP en el iDRAC6 se debe definir de manera que coincida con la misma dirección FQDN para que la validación del certificado funcione.

5 En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrarlo.

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.

6 Haga clic en **Cargar**.

El certificado de la CA raíz que firma todos los certificados de servidores de capa de sockets seguros (SSL) de los controladores de dominio ha sido cargado.

7 Haga clic en **Siguiente**. Aparece la página **Paso 2 de 3** de **Configuración y administración de LDAP genérico**. Use esta página para configurar la información de ubicación de los servidores de LDAP genérico y las cuentas de los usuarios.

NOTA: En esta versión, las funciones de autentificación de dos factores (TFA) basada en tarjeta inteligente e inicio de sesión único (SSO) no se admiten para el servicio de directorio de LDAP genérico.

8 Introduzca la información siguiente:

- Seleccione la opción **Activar LDAP genérico**.

NOTA: En esta versión no se admite el grupo anidado. El firmware busca al miembro directo del grupo para que coincida con el DN del usuario. Además, sólo se admite un dominio único. No se admiten dominios cruzados.

- Seleccione la opción **Usar nombre distinguido para buscar la pertenencia a grupos** para emplear el nombre distinguido (DN) como miembros del grupo. iDRAC6 compara el DN del usuario recuperado del directorio para compararlo con los miembros del grupo. Si esta opción no está seleccionada, el nombre de usuario proporcionado por el usuario se utiliza para compararlo con los miembros del grupo.
- En el campo **Dirección del servidor LDAP**, introduzca el nombre de dominio completo o la dirección IP del servidor LDAP. Para especificar múltiples servidores LDAP redundantes que sirven al mismo dominio, proporcione la lista de todos los servidores separados por comas. iDRAC6 intenta conectar a cada servidor, uno por uno, hasta que logra una conexión satisfactoria.
- Introduzca el puerto usado por el LDAP a través de SSL en el campo **Puerto del servidor LDAP**. El valor predeterminado es 636.
- En el campo **DN de enlace**, introduzca el DN de un usuario utilizado para enlazar al servidor durante la búsqueda del DN del usuario. Si no está especificado, se utiliza un enlace anónimo.
- Introduzca la **Contraseña de enlace** para usarla junto con el **DN de enlace**. Esta opción es obligatoria si no se admite el enlace anónimo.

- En el campo **DN de base para buscar**, introduzca el DN del subdirectorio donde deben iniciarse todas las búsquedas.
- En el campo **Atributo de inicio de sesión del usuario**, introduzca el atributo del usuario a buscar. El valor predeterminado es UID. Se recomienda que este nombre sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar la singularidad del usuario. Si el DN del usuario no puede ser identificado en forma exclusiva por la combinación de búsqueda de atributo y filtro de búsqueda, el inicio de sesión falla.
- En el campo **Atributo de pertenencia a grupo**, especifique qué atributo de LDAP debe utilizarse para verificar la pertenencia al grupo. Éste debe ser un atributo de la clase de grupos. Si no está especificado, iDRAC6 usa los atributos de *miembro* y *miembro único*.
- En el campo **Filtro de búsqueda**, introduzca un filtro de búsqueda de LDAP válido. Use el filtro si el atributo del usuario no logra identificar de forma exclusiva al usuario dentro del DN de base seleccionado. Si no está especificado, el valor predeterminado es *objectClass*=*, que busca todos los objetos en el árbol. Este filtro de búsqueda adicional configurado por el usuario se aplica únicamente para la búsqueda de DN del usuario y no para la búsqueda de pertenencia de grupo.

9 Haga clic en **Siguiente**. Aparece la página **Paso 3a de 3** de **Configuración y administración de LDAP genérico**. Use esta página para configurar los grupos de privilegios utilizados para autorizar a los usuarios. Al activar el LDAP genérico, se usan grupos de funciones para especificar la política de autorización para los usuarios de iDRAC6.

NOTA: En esta versión, a diferencia de AD, no es necesario usar caracteres especiales ("@", "\" y "/") para distinguir un usuario de LDAP de un usuario local. Sólo hace falta introducir el nombre de usuario para iniciar sesión, y no se debe introducir el nombre de dominio.

10 En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

Aparece la página **Paso 3b de 3 de** Configuración y administración de LDAP genérico. Use esta página para configurar cada grupo de funciones empleado para controlar la política de autorizaciones de los usuarios.

11 En el campo **DN de grupo**, introduzca el nombre distintivo del grupo que identifica al grupo de funciones en el servicio de directorio de LDAP genérico asociado con el iDRAC6.

12 En la sección **Privilegios del grupo de funciones**, especifique los privilegios asociados con el grupo seleccionando la opción **Nivel de privilegio del grupo de funciones**. Por ejemplo, si selecciona **Administrador**, se seleccionan todos los privilegios para dicho nivel de permiso.

13 Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.

El servidor web del iDRAC6 regresa automáticamente a la página **Paso 3a de 3 de Configuración y administración de LDAP genérico**, donde se muestra la configuración del grupo de funciones.

14 Configure grupos de funciones adicionales, si es necesario.

15 Haga clic en **Terminar** para regresar a la página de resumen de **Configuración y administración de LDAP genérico**.

16 Haga clic en **Comprobar configuración** para verificar la configuración del LDAP genérico.

17 Escriba el nombre de usuario y la contraseña de un usuario del directorio seleccionado para comprobar la configuración del LDAP. El formato depende del *Atributo de inicio de sesión del usuario* que se utilice, y el nombre de usuario introducido debe coincidir con el valor del atributo seleccionado.

Aparecen los resultados de la prueba y el registro de la misma. Ha terminado la configuración del servicio de directorio de LDAP genérico.

Configuración del servicio de directorio LDAP genérico mediante RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1

racadm config -g cfgldap -o cfgLdapServer <FQDN o
dirección_IP>

racadm config -g cfgldap -o cfgLdapPort <Número de
puerto>

racadm config -g cfgldap -o cfgLdapBaseDN
dc=common,dc=com
```

```
racadm config -g cfgldap -o
cfgLdapCertValidationenable 0
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone,ou=groups,
dc=common,dc=com'
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

Ver la configuración por medio de los comandos que se muestran a continuación

```
racadm getconfig -g cfgldap
```

```
racadm getconfig -g cfgldaprolegroup -i 1
```

Utilice RACADM para confirmar si es posible iniciar sesión

```
racadm -r <IP_de_iDRAC6> -u user.1 -p password
getractime
```

Configuración adicional para probar la opción BindDN

```
racadm config -g cfgldap -o cfgLdapBindDN
"cn=idrac_admin,ou=iDRAC_admins,ou=People,
dc=common,dc=com"
```

```
racadm config -g cfgldap -o cfgLdapBindPassword
password
```

NOTA: Configure el iDRAC6 para usar un servidor de nombre de dominio, que descifre el nombre de host del servidor LDAP que iDRAC6 tiene configurado para usar en la dirección del servidor LDAP. El nombre de host debe coincidir con el "CN" o "Asunto" en el certificado del servidor LDAP.

Preguntas frecuentes acerca de Active Directory

No puedo iniciar sesión en Active Directory. ¿Cómo puedo solucionar el 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 **Configuración de iDRAC→ ficha Red/seguridad→ Servicio de directorio→ Microsoft 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. Regrese 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 vuelva a ejecutar la prueba 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 de usuario y los resultados de la prueba muestran el siguiente mensaje de error:

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 periodo 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 la 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 periodo válido del certificado del servidor o del certificado de CA. Verifique la hora del iDRAC6 y el periodo 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 del 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.

Estoy usando un esquema extendido en un entorno de dominios múltiples. ¿Cómo configuro las direcciones de controladores de dominio?

Debe usar el nombre del host (FQDN) o la dirección IP de los controladores de dominio que sirven al dominio donde reside el objeto iDRAC6.

¿Cuándo necesito configurar una dirección de catálogo global?

Si utiliza un esquema extendido, no se utiliza la dirección de catálogo global.

Si utiliza 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 enlaza a LDAP a través de una conexión insegura.

¿Por qué el iDRAC6 activa la validación de certificados de manera 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 de su límite de seguridad sin validación de certificado, puede desactivarla por medio de la interfaz gráfica del usuario o la interfaz de línea de comandos.

¿Admite el iDRAC6 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 de la siguiente manera: haga 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, ver "Prueba de las configuraciones realizadas" en la página 193.

La mayoría de los problemas se explican en esta sección; sin embargo, por lo general debe verificar lo siguiente:

1. Compruebe que está usando el nombre de dominio de usuario correcto durante el 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 seleccionado la opción **Habilitar Active Directory** en la página **Configuración y administración 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 la hora del iDRAC6 se encuentre dentro del periodo de validez del certificado de CA.

   d. Si está utilizando el esquema extendido, 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 **Nombre del grupo** y **Nombre de dominio del grupo** coincidan con la configuración de Active Directory.

3. Verifique los certificados SSL del controlador de dominio para asegurarse de que la hora del iDRAC6 está dentro del plazo de vigencia del certificado.

8

Configuración del iDRAC6 para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

Esta sección brinda información para configurar iDRAC6 para iniciar sesión mediante tarjeta inteligente para usuarios locales y usuarios de Active Directory, y para el inicio de sesión único (SSO) para usuarios de Active Directory.

iDRAC6 admite la autentificación de Active Directory con Kerberos para permitir el inicio de sesión único (SSO) y con tarjeta inteligente en Active Directory.

Acerca de la autentificación basada en Kerberos

Kerberos es un protocolo de autentificación 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 la autentificación, el iDRAC6 ahora admite la autentificación 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 usan Kerberos como su método de autentificación predeterminado.

El iDRAC6 utiliza Kerberos para admitir dos tipos de mecanismos de autentificación: el inicio de sesión único y con tarjeta inteligente en Active Directory. Para el inicio de sesión único de Active Directory, el iDRAC6 utiliza las credenciales de usuario almacenadas en caché en el sistema operativo después de que el usuario ha iniciado sesión usando una cuenta válida de Active Directory.

Para el inicio de sesión con tarjeta inteligente de Active Directory, el iDRAC6 utiliza la autentificación de dos factores (TFA) con tarjeta inteligente a modo de credenciales para permitir el inicio de sesión en Active Directory. Esta es la función siguiente a la autentificación mediante tarjeta inteligente local.

La autentificación de Kerberos en el iDRAC6 falla si la hora del iDRAC6 difiere de la hora del controlador de dominio. Se permite una diferencia máxima de 5 minutos. Para permitir una autentificación correcta, sincronice la hora del servidor con la hora del controlador de dominio y después **restablezca** el iDRAC6.

Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory

Los prerrequisitos tanto para el inicio de sesión único como para la autentificación mediante tarjeta inteligente de Active Directory son:

- Configure el iDRAC6 para el inicio de sesión de Active Directory. Para obtener más información, consulte "Uso del servicio de directorio del iDRAC6" en la página 155.
- Registre el iDRAC6 como equipo en el dominio raíz de Active Directory. Para hacer esto:
  - **a** Haga clic en **Configuración del iDRAC**→ ficha **Red/Seguridad**→ subficha **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 autentifica las cuentas de Active Directory de los usuarios.
  - **c** Seleccione **Registrar el iDRAC en DNS**.
  - **d** Indique 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 autentificación, el iDRAC6 admite la configuración para activarse como si fuera un servicio de Kerberos en una red Kerberos de Windows. 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) a 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 contiene 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 autentificación 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 de carga y se activa para actuar como si fuera un servicio de Kerberos en la red.

Como el iDRAC6 es un dispositivo con un sistema operativo que no es Windows, ejecute la utilidad **ktpass** (que es 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** siguiente 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 autentificación con Kerberos es DES-CBC-MD5. El tipo principal es KRB5_NT_PRINCIPAL. Las propiedades de la cuenta del usuario a la que está asignado el nombre principal de servicio deben tener activada la propiedad **Utilizar los tipos de cifrado DES para esta cuenta**.

NOTA: Se recomienda usar la utilidad **ktpass** más reciente para crear el archivo keytab.

Este procedimiento genera un archivo keytab que se debe cargar en el iDRAC6.

NOTA: Este archivo contiene una clave de cifrado y debe guardarse 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. También puede utilizar el siguiente comando de diferencia de zona horaria de RACADM para sincronizar la hora:

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset <offset value>
  ```

- Para activar el inicio de sesión único en el esquema extendido, asegúrese de que la opción **Confiar en este usurario para delegar a cualquier servicio (sólo Kerberos)** esté seleccionada en la ficha **Delegación** para el usuario de keytab. Esta ficha está disponible sólo después de crear el archivo keytab con la utilidad **ktpass**.

Configuración del explorador para activar el inicio de sesión único de Active Directory

Para configurar los valores del explorador para Internet Explorer:

1. Abra el explorador de web Internet Explorer.
2. Seleccione **Herramientas→ Opciones de Internet→ Seguridad→ Intranet local**.
3. Haga clic en **Sitios**.
4. Seleccione las siguientes opciones solamente:
   - Incluya todos los sitios locales (intranet) no enumerados en otras zonas.
   - Incluya todos los sitios que omiten el servidor proxy.
5. Haga clic en **Advanced** (Opciones avanzadas).
6. Agregue todos los nombre de dominio relativos que se utilizarán para las instancias de Weblogic Server que son parte de la configuración del inicio de sesión único (por ejemplo, mihost.ejemplo.com).
7. Haga clic en **Cerrar** y luego en **Aceptar**.
8. Haga clic en **OK** (Aceptar).

Para configurar los valores del explorador para Firefox:

1. Abra el explorador de web Firefox.
2. En la barra de dirección, introduzca `about:config`.
3. En **Filtro**, introduzca `network.negotiate`.
4. Agregue el nombre del iDRAC a network.negotiate-auth.trusted-uris (mediante una lista separada con comas).
5. Agregue el nombre del iDRAC a network.negotiate-auth.delegation-uris (mediante una lista separada con comas).

Uso del inicio de sesión único de Microsoft Active Directory

La función de inicio de sesión único permite iniciar sesión directamente en el iDRAC6 después de conectarse a la estación de trabajo sin necesidad de introducir credenciales de autentificación 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, deberá haber configurado la cuenta de usuario para iniciar sesión en el iDRAC6 con las credenciales de Active Directory. El iDRAC6 usa las credenciales de Active Directory guardadas en la caché para iniciar la sesión.

Se puede activar el iDRAC6 para usar Kerberos (un protocolo de autentificación de red) para activar el inicio de sesión único. Para obtener más información, consulte "Acerca de la autentificación basada en Kerberos" en la página 205. Asegúrese de haber realizado los pasos enumerados en la sección "Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory" en la página 206 antes de configurar el iDRAC6 para el inicio de sesión único.

Configuración del iDRAC6 para utilizar el inicio de sesión único

Lleve a cabo los siguientes pasos para configurar el iDRAC6 para el inicio de sesión único mediante la interfaz web del iDRAC:

1. Inicie sesión en la interfaz web del iDRAC.
2. Vaya a **Configuración del iDRAC**→ ficha **Red/Seguridad**→ ficha **Servicio de directorio**→ **Microsoft Active Directory**.

3 Haga clic en **Configurar Active Directory**. Aparece la página **Paso 1 de 4 de Configuración y administración de Active Directory**.

4 Cargue el archivo keytab obtenido del dominio raíz de Active Directory, en el iDRAC6. Para hacerlo, en **Cargar archivo keytab de Kerberos**, escriba la ruta de acceso del archivo keytab o haga clic en **Examinar** para ubicar el archivo. Haga clic en **Cargar**. El archivo keytab de Kerberos se cargará en el iDRAC6. El archivo keytab es el mismo archivo que se creó al realizar las tareas enumeradas en "Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory" en la página 206.

5 Haga clic en **Siguiente**. Aparece la página **Paso 2 de 4** de **Configuración y administración de Active Directory**.

6 Seleccione **Activar el inicio de sesión único** para activar el inicio de sesión único.

7 Haga clic en **Siguiente** hasta que aparezca la última página. Si Active Directory está configurado para utilizar el esquema estándar, aparece la página **Paso 4a de 4** de **Configuración y administración de Active Directory**. Si Active Directory está configurado para utilizar el esquema extendido, aparece la página **Paso 4 de 4** de **Configuración y administración de Active Directory**.

8 Haga clic en **Terminar** para aplicar la configuración.

Uso de RACADM:

Se puede cargar el archivo keytab en el iDRAC6 con el siguiente comando de la interfaz de línea de comandos de racadm:

```
racadm krbkeytabupload -f <filename>
```

donde <filename> es el nombre del archivo keytab. El comando racadm es compatible con racadm local y remota.

Para activar la función de inicio de sesión único por medio de la interfaz de línea de comandos, ejecute el siguiente comando racadm:

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Inicio de sesión en iDRAC6 mediante inicio de sesión único

1. Inicie sesión en el sistema usando una cuenta de Active Directory válida.
2. Para acceder a la página web del iDRAC6, escriba lo siguiente:

   `https://<dirección FQDN>`

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

   `https://<dirección FQDN>:<número de puerto>`

   donde *dirección FQDN* es el FQDN de iDRAC (nombre dns de idrac.nombre de dominio) y *número de puerto* es el número de puerto HTTPS.

   NOTA: Si se usa la dirección IP en lugar del FQDN, el inicio de sesión único falla.

   El iDRAC6 inicia 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.

   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 autentificación de Active Directory con Kerberos.

Configuración de la autentificación de tarjeta inteligente

El iDRAC6 admite la función de autentificación de dos factores (TFA) si se activa el **Inicio de sesión mediante tarjeta inteligente**.

Los esquemas tradicionales de autentificación utilizan nombres de usuario y contraseñas para autentificar a los usuarios. Esto proporciona una seguridad mínima.

En cambio, la función TFA brinda mayor seguridad porque los usuarios deben proporcionar dos factores de autentificación, el que poseen y el que conocen. El factor que se posee es la tarjeta inteligente, un dispositivo físico, y el factor que se conoce es un código secreto, como una contraseña o PIN.

La autentificación de dos factores requiere que los usuarios verifiquen su identidad cuando proporcionan *ambos* factores.

Configuración de usuarios de iDRAC6 locales para Inicio de sesión mediante tarjeta inteligente

Puede configurar que los usuarios iDRAC6 locales inicien sesión en el iDRAC6 usando la tarjeta inteligente. Haga clic en **Configuración del iDRAC→ Red/Seguridad→ Usuarios**.

Sin embargo, antes de que el usuario pueda iniciar sesión en el iDRAC6 con la tarjeta inteligente, debe cargar el certificado de tarjeta inteligente del usuario y el certificado de la autoridad de certificados (CA) de confianza para certificar el iDRAC6.

NOTA: Compruebe que la validación del certificado de CA esté activada antes de configurar la tarjeta inteligente.

Exportación del certificado de tarjeta inteligente

Puede obtener el certificado del usuario exportando el certificado de tarjeta inteligente con el software de administración de tarjetas (CMS), de la tarjeta inteligente a un archivo en formato codificado Base64. Habitualmente, el CMS puede obtenerse del proveedor de la tarjeta inteligente. Este archivo codificado se debe cargar en el iDRAC6 como certificado del usuario. 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 Base 64. 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, "sampleuser@domain.com", el nombre de usuario deberá configurarse como "sampleuser".

Configuración de usuarios de Active Directory para Inicio de sesión mediante tarjeta inteligente

Antes de usar la función de inicio de sesión mediante tarjeta inteligente de Active Directory, compruebe que el iDRAC6 ya está configurado para el inicio de sesión de Active Directory y 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. Ver "Uso del servicio de directorio del iDRAC6" en la página 155 para obtener más información sobre cómo configurar los 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.

Para configurar los usuarios de Active Directory para que inicien sesión en el iDRAC6 usando 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. Ver "Uso del servicio de directorio del iDRAC6" en la página 155 para obtener más información sobre cómo configurar los usuarios de Active Directory.

Puede configurar Active Directory en **Configuración del iDRAC→ Red/Seguridad→ Servicio de directorio→ Microsoft Active Directory.**

NOTA: Compruebe que la validación del certificado de CA esté activada antes de configurar la tarjeta inteligente.

Configuración de la tarjeta inteligentee mediante iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

1. En la interfaz web del iDRAC6, vaya a **Configuración del iDRAC→ Red/Seguridad→** ficha **Tarjeta inteligente**.
2. Configure los valores de Inicio de sesión mediante tarjeta inteligente.

   La Tabla 8-1 contiene información sobre los valores de la página **Tarjeta inteligente**.
3. Haga clic en **Aplicar**.

Tabla 8-1. Valores de la tarjeta inteligente

Valor	Descripción
Configurar Inicio de sesión mediante tarjeta inteligente	• **Desactivado**: desactiva el Inicio de sesión mediante tarjeta inteligente. Los subsiguientes inicios de sesión 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, mantienen el estado correspondiente. • **Activado**: Activa el Inicio de sesión mediante tarjeta inteligente. Después de aplicar los cambios, desconéctese, inserte su tarjeta inteligente y haga clic en **Iniciar sesión** para introducir el PIN de la tarjeta inteligente. La activación del inicio de sesión mediante tarjeta inteligente desactiva todas las interfaces de línea de comandos fuera de banda, incluyendo SSH, Telnet, serie, racadm remota e IPMI en la LAN, ya que estos servicios sólo admiten la autentificación de un solo factor. • **Activado con racadm remota**: activa el Inicio de sesión mediante tarjeta inteligente junto con RACADM remota. Todas las demás interfaces fuera de banda de la CLI se desactivan. Si se selecciona **Activado** o **Activado con racadm remota**, se le solicita que inicie sesión mediante tarjeta inteligente en cada intento de inicio de sesión subsiguiente usando la interfaz web. Se recomienda que el administrador del iDRAC6 utilice la opción **Activar con racadm remota** únicamente para acceder a la interfaz web del iDRAC6, para ejecutar secuencias de comandos con los comandos de racadm remota. Si el administrador no necesita usar racadm remota, se recomienda usar la opción **Activado** para el inicio de sesión mediante tarjeta inteligente. 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 mediante tarjeta inteligente. **NOTA:** El Inicio de sesión mediante tarjeta inteligente requiere que se configuren los usuarios locales del iDRAC6 con los certificados correspondientes. Si se utiliza el Inicio de sesión mediante tarjeta inteligente para que un usuario de Microsoft Active Directory inicie sesión, debe asegurarse de configurar el certificado de usuario de Active Directory para dicho usuario. Puede configurar el certificado de usuario en la página **Usuarios→ iMenú principal de usuario**.

Tabla 8-1. Valores de la tarjeta inteligente *(continuación)*

Valor	Descripción
Activar la revisión CRL para el Inicio de sesión mediante tarjeta inteligente	Esta revisión 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. Se verifica si el certificado de iDRAC del usuario, que se descarga del servidor de distribución de la lista de revocación de certificados (CRL), ha sido revocado en la lista. Los servidores de distribución de CRL aparecen en los certificados de tarjeta inteligente de los usuarios. 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 del iDRAC6 en **Configuración del iDRAC→ Red/Seguridad→ 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 **Red/Seguridad→ Red** para que esta comprobación se realice correctamente.

Inicio de sesión en el iDRAC6 usando la tarjeta inteligente

La interfaz web del iDRAC6 muestra la página de Inicio de sesión mediante tarjeta inteligente de todos los usuarios 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 estén completas antes de activar el Inicio de sesión mediante tarjeta inteligente.

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 Entre 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.

Aparece la página Inicio de sesión del iDRAC6 y le solicita que inserte la tarjeta inteligente.

2 Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.

El iDRAC6 solicita 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 es un usuario de Active Directory para quien se ha seleccionado la opción **Activar la revisión CRL para el Inicio de sesión mediante 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 autentificación 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.

Aparece la página Inicio de sesión del iDRAC6 y le solicita 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**.

Ha iniciado sesión en el iDRAC6 con sus credenciales, como están definidas en Active Directory.

Solución de problemas de inicio de sesión mediante tarjeta inteligente en el iDRAC6

Utilice las siguientes sugerencias para depurar una tarjeta inteligente que no permite el acceso:

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Verifique que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows. Windows admite una cantidad limitada de proveedores de servicios de cifrado (CSP) de tarjetas inteligente.

Sugerencia: 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 esa tarjeta 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, compruebe si el nombre de usuario y los certificados de usuario que están cargados en el iDRAC6 han caducado. Los registros de rastreo del iDRAC6 pueden proporcionar importantes mensajes de registro sobre los errores; a pesar de que 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, intente iniciar sesión en el iDRAC6 sin activar el Inicio de sesión mediante tarjeta inteligente. Si ha activado la revisión de CRL, intente iniciar sesión en Active Directory sin activar la revisión de CRL. El registro de rastreo de iDRAC6 debería proporcionar importantes mensajes si se presenta algún error de CRL.
- También tiene la opción de desactivar el Inicio de sesión mediante tarjeta inteligente por medio de la racadm local con el siguiente comando: `racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0`
- En las plataformas Windows de 64 bits, no se instala el complemento Active-X de autentificación del iDRAC6 si se implementó una versión de 64 bits del Paquete redistribuible de Microsoft Visual C++ 2005. Para instalar y ejecutar el complemento Active-X correctamente, implemente la versión de 32 bits del Paquete redistribuible de Microsoft Visual C++ 2005 SP1 (x86). Este paquete es necesario para ejecutar la sesión de consola virtual en un explorador Internet Explorer.
- Si recibe el siguiente mensaje de error "`No es posible cargar el complemento de tarjeta inteligente. Verifique la configuración de IE o podría tener privilegios insuficientes para usar el complemento de tarjeta inteligente`", luego instale el Paquete redistribuible de Microsoft Visual C++ 2005 SP1 (x86). Este archivo está disponible en el sitio web de Microsoft en **microsoft.com**. Se han probado dos versiones distribuidas del paquete redistribuible de C++, las cuales permiten que se cargue el complemento de tarjeta inteligente de Dell. Consulte Tabla 8-2 para obtener información detallada.

Tabla 8-2. Versiones distribuidas del paquete redistribuible de C++

Nombre de archivo del paquete redistribuible	Version (Versión)	Fecha de publicación	Tamaño	Descripción
vcredist_x86.exe	6.0.2900.2180	21 de marzo de 2006	2.56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	7 de noviembre de 2007	1.73 MB	Redistribuible 2008 de Microsoft

- Asegúrese de que la hora del iDRAC6 y la del controlador de dominio en el servidor del controlador de dominio estén configuradas con 5 minutos o menos de diferencia entre sí para que funcione la autentificación con Kerberos. Consulte la **Hora del RAC** en la página **Sistema→ Configuración del iDRAC→ Propiedades→ Información de iDRAC**, y la hora del controlador de dominio, haciendo clic con el botón derecho del mouse en la hora que se encuentra en la esquina inferior derecha de la pantalla. La diferencia de zona horaria se muestra en el cuadro emergente. Para la hora estándar de la zona central (CST) de los EE. UU., la diferencia es –6. Use el siguiente comando RACADM de diferencia de zona horaria para sincronizar la hora del iDRAC6 (mediante racadm remota o racadm Telnet/SSH): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <valor de la diferencia en minutos>.` Por ejemplo, si la hora del sistema es GMT -6 (CST de los EE.UU.) y la hora es 2 p.m., establezca la hora del iDRAC6 en las 18.00 horas GMT, y debería introducir 360 en el comando anterior para especificar la diferencia. También puede usar *cfgRacTuneDaylightoffset* para activar la variación de horario de verano. Esto evita tener que cambiar la hora dos veces al año cuando se realizan los ajustes de horario de verano, o simplemente calcúlelo en la diferencia anterior usando 300 en el ejemplo que antecede.

Preguntas frecuentes acerca del inicio de sesión único

El inicio de sesión único falla en Windows Server 2008 R2 x64. ¿Qué debo hacer para que el inicio de sesión único funcione con Windows Server 2008 R2 x64?

1. Ejecute **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** para el controlador de dominio y la política de dominio. Configure los equipos para usar el paquete de cifrado DES-CBC-MD5. Esta configuración puede afectar la compatibilidad con equipos clientes o con los servicios y aplicaciones del entorno. El valor de la política **Configurar tipos de cifrado permitidos para Kerberos** se encuentra en **Configuración del equipo\Configuración de seguridad\Políticas locales\Opciones de seguridad**.

2. Es necesario que los clientes de dominio tengan el GPO actualizado. En la línea de comandos, escriba `gpupdate/force` y elimine el archivo keytab antiguo con el comando `klist purge`.
3. Una vez que GPO ha sido actualizado, cree el nuevo archivo keytab.
4. Cargue el archivo keytab en el iDRAC6.

Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

El inicio de sesión único falla en el caso de usuarios de AD en Windows 7 y Windows Server 2008 R2. ¿Qué debo hacer para resolver esto?

Debe activar los tipos de cifrado para Windows 7 y Windows Server 2008 R2. Para activar los tipos de cifrado:

1. Inicie sesión como administrador o como usuario con privilegios administrativos.
2. Vaya a **Inicio** y ejecute **gpedit.msc**. Aparece la ventana **Editor de políticas de grupo local**.
3. Acceda a **Configuración del equipo local→ Configuración de Windows→ Configuración de seguridad→ Políticas locales→ Opciones de seguridad**.
4. Haga clic con el botón derecho del mouse en **Seguridad de la red: Configuración de los tipos de cifrado permitidos para Kerberos** y seleccione **Propiedades**.
5. Active todas las opciones.
6. Haga clic en **OK** (Aceptar). Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

Indique los siguientes valores adicionales para el esquema extendido:

1. En la ventana **Editor de políticas de grupo local**, acceda a **Configuración del equipo local→ Configuración de Windows→ Configuración de seguridad→ Políticas locales→ Opciones de seguridad**.
2. Haga clic con el botón derecho del mouse en **Seguridad de la red: Restricción de NTLM: Tráfico de NTLM de salida al servidor remoto** y seleccione **Propiedades**.
3. Seleccione **Permitir todas**.
4. Haga clic en **Aceptar** y luego cierre la ventana **Editor de políticas de grupo local**.
5. Vaya a **Inicio** y ejecute **cmd**. Aparece la ventana del **símbolo del sistema**.

6. Ejecute el comando `gpupdate /force`. Las políticas de grupo se actualizan. Cierre la ventana del **símbolo del sistema**.
7. Vaya a **Inicio** y ejecute **regedit**. Aparece la ventana **Editor del registro**.
8. Acceda a **HKEY_LOCAL_MACHINE→ Sistema→ Establecer control actual→ Control→ LSA**.
9. En el panel derecho, haga clic con el botón derecho del mouse y seleccione **Nuevo→ Valor de DWORD (32 bits)**.
10. Asigne a la nueva clave el nombre **Suprimir protección extendida**.
11. Haga clic con el botón derecho del mouse en **Suprimir protección extendida** y haga clic en **Modificar**.
12. En el campo **Datos de valor**, escriba 1 y haga clic en **Aceptar**.
13. Cierre la ventana **Editor del registro**. Ahora puede iniciar sesión en el iDRAC mediante el inicio de sesión único.

Si ha activado el inicio de sesión único para iDRAC y está utilizando Internet Explorer para iniciar sesión en el iDRAC, el inicio de sesión único falla y le solicita que introduzca su nombre de usuario y contraseña. ¿Cómo resuelvo esto?

Compruebe que la dirección IP del iDRAC figure en **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza**. Si no figura, el inicio de sesión único falla y le solicita que introduzca su nombre de usuario y contraseña. Haga clic en **Cancelar** y continúe.

9

Uso de la consola virtual de la interfaz gráfica de usuario

Esta sección proporciona información acerca de cómo usar la función de consola virtual del iDRAC6.

Descripción general

La función de consola virtual del iDRAC6 le permite tener acceso a la consola local de manera remota en modo de gráficos o de texto. Mediante la consola virtual, 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 cambio se pueden administrar los servidores desde cualquier punto, un equipo de escritorio o un equipo portátil. También se puede compartir información con terceros de manera remota e instantánea.

Uso de la consola virtual

NOTA: Al abrir una sesión de consola virtual, el servidor administrado no indica que la consola ha sido redirigida.

NOTA: Si hay una sesión de consola virtual abierta desde la estación de administración a un iDRAC6 concreto, cualquier intento de abrir una sesión nueva desde la misma estación de administración a ese iDRAC6 fallará.

NOTA: Es posible abrir varias sesiones de consola virtual desde una sola estación de administración hacia múltiples controladores del iDRAC6 simultáneamente.

La página **Consola virtual** permite administrar el sistema remoto mediante el teclado, vídeo y mouse de la estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta función se puede usar junto con la función de medios virtuales para realizar instalaciones de software remotas.

Las siguientes reglas se aplican a una sesión de consola virtual:

- Se admite un máximo de cuatro sesiones de consola virtual simultáneas. Todas las sesiones muestran la misma consola de servidor administrado simultáneamente.
- A partir de la versión 1.5, es posible abrir varias sesiones en varios servidores remotos desde el mismo cliente, según el orden en el que se van abriendo. Si se abre una sesión de consola virtual mediante el complemento de Java, se puede abrir otra sesión de consola virtual mediante el complemento de ActiveX. Sin embargo, si se abre una sesión de consola virtual mediante ActiveX, no se puede abrir otra sesión de consola virtual mediante el complemento de Java. Se debe cerrar la primera sesión de consola virtual para abrir una segunda sesión.
- La sesión de consola virtual no se debe ejecutar desde un explorador web del sistema administrado.
- Debe haber disponible un ancho de banda de red de al menos 1 MB/s.
- La primera sesión de consola virtual hacia el iDRAC6 es una sesión de acceso total. Si un segundo usuario solicita una sesión de consola virtual, se notifica al primer usuario y se le da la opción (aprobar, rechazar o permitir como sólo lectura) de enviar una solicitud para compartir al segundo usuario. El segundo usuario es notificado de que otro usuario tiene el control. Cuando el primer usuario no responde a la solicitud para compartir de cada usuario subsiguiente en un plazo de tiempo de espera de 30 segundos, el acceso a la consola virtual se otorga con base en el valor establecido para el objeto `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions`. Este objeto es independiente del tipo de complemento (ActiveX o Java) establecido para utilizarse en la segunda/tercera/cuarta sesión. Para obtener más información sobre este objeto, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia de Dell Support en **dell.com/support/manuals**.

  NOTA: Esta regla se aplica sólo con el RACADM remoto o del firmware (SSH o Telnet), y no con el RACADM local.

Configuración de la estación de administración

Para usar la consola virtual 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" en la página 28
   - "Configuración de un explorador web admitido" en la página 46
2. Si usa Firefox o desea usar el visor de Java con Internet Explorer, instale Java Runtime Environment (JRE). Si usa el explorador Internet Explorer, se ofrece un control ActiveX para el visor de consola. También puede usar el visor de consola de Java con Firefox si instala JRE y configura el visor de consola en la interfaz web del iDRAC6 antes de iniciar el visor.
3. Si utiliza Internet Explorer (IE), compruebe que el explorador esté activado para descargar contenido cifrado, como se indica a continuación:
   - Desde Internet Explorer, vaya a Opciones o Configuración y seleccione **Herramientas→ Opciones de Internet→ Opciones avanzadas**.
   - Desplácese hasta la sección **Seguridad** y deseleccione esta opción:

     `No guardar las páginas cifradas en el disco.`
4. Si va a usar Internet Explorer para iniciar una sesión de consola virtual con el complemento de ActiveX, asegúrese de haber agregado el IP del iDRAC6 o el nombre de host en la lista de **Sitios de confianza**. También debe restablecer la configuración personalizada como **Media baja** o cambiar los valores para permitir la instalación de los complementos ActiveX. Para obtener más información, consulte "Configuraciones del explorador Internet Explorer para aplicaciones de consola virtual y de medios virtuales con ActiveX" en la página 227.

NOTA: El complemento ActiveX de 64 bits no se admite para iniciar una sesión de consola virtual mediante Internet Explorer.

5 Se recomienda configurarla resolución del monitor en 1280 x 1024 píxeles o más.

NOTA: Si el sistema ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Presione <Ctrl><Alt><F1> en la consola virtual del iDRAC6 para cambiar Linux a consola de texto.

NOTA: Ocasionalmente, puede encontrar el siguiente error de compilación de Java Script: "`Esperado: ;`". Para resolver este problema, ajuste la configuración de red para utilizar **Conexión directa** en JavaWebStart: **Editar**→ **Preferencias**→ **General**→ **Configuración de red** y elija **Conexión directa** en lugar de **Utilizar configuración del explorador**.

Limpiar el caché del explorador

Si tiene problemas para usar la consola virtual (errores de fuera de rango, problemas de sincronización, etc.) borre la caché del explorador para quitar o eliminar las versiones anteriores del visor que pudieran estar almacenadas en el sistema e inténtelo nuevamente.

NOTA: Debe tener privilegios de administrador para borrar la caché del explorador.

Para borrar versiones anteriores del visor de Active-X para IE7, haga lo siguiente:

1 Cierre el Video Viewer y el explorador de Internet Explorer.

2 Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer**→ **Herramientas**→ **Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.

3 Seleccione **Complementos utilizados por Internet Explorer** en el menú desplegable **Mostrar**.

4 Elimine el complemento *Video Viewer*.

Para limpiar las versiones anteriores del visor Active-X para IE8, haga lo siguiente:

1 Cierre el Video Viewer y el explorador de Internet Explorer.

2 Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer**→ **Herramientas**→ **Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.

3 Seleccione **Todos los complementos** en el menú desplegable **Mostrar**.

4 Seleccione el complemento *Video Viewer* y haga clic en el vínculo **Más información**.

5 Seleccione **Quitar** de la ventana **Más información**.

6 Cierre las ventanas **Más información** y **Administrar complementos**.

Para borrar las versiones anteriores del visor de Java en Windows o Linux, haga lo siguiente:

1 En el indicador de comandos, ejecute `javaws-viewer` o `javaws-uninstall`

2 Aparece el **Visor de la caché de Java**.

3 Elimine los elementos con el título *Cliente de consola virtual de iDRAC6*.

Configuraciones del explorador Internet Explorer para aplicaciones de consola virtual y de medios virtuales con ActiveX

En esta sección se proporciona información acerca de la configuración del explorador Internet Explorer requerida para iniciar y ejecutar aplicaciones de consola virtual y de medios virtuales basadas en ActiveX.

NOTA: Borre la caché del explorador y luego introduzca los valores de configuración del explorador. Para obtener más información, consulte "Limpiar el caché del explorador" en la página 226.

Valores comunes para los sistemas operativos Microsoft Windows

1 En Internet Explorer, vaya a la ficha **Herramientas→ Opciones de Internet→ Seguridad**.

2 Seleccione la Zona que desea utilizar para ejecutar la aplicación.

3 Haga clic en **Personalizar**. Si está utilizando Internet Explorer 8, haga clic en **Nivel personalizado**. Aparece la ventana **Configuración de seguridad**.

4 En **Controles y complementos de ActiveX**:

- Seleccione la opción **Preguntar** para **Descargar controles ActiveX firmados**
- Seleccione la opción **Habilitar** o **Preguntar** para **Ejecutar controles y complementos de ActiveX**
- Seleccione la opción **Habilitar** o **Preguntar** para **Generar scripts de los controles ActiveX marcados como seguros para scripts**
- Haga clic en **Aceptar** y luego vuelva a hacer clic en **Aceptar**.

Valores adicionales para los sistemas operativos de Microsoft Windows Vista o más recientes

Los exploradores Internet Explorer en los sistemas operativos Windows Vista o más recientes tienen una función de seguridad adicional denominada "Modo protegido".

Puede iniciar y ejecutar aplicaciones de ActiveX en exploradores Internet Explorer con "Modo protegido" de una de las siguientes maneras:

- Vaya a **Archivos de programa→ Internet Explorer**. Haga clic con el botón derecho del mouse en **iexplore.exe** y haga clic en **Ejecutar como administrador**.
- Agregue la dirección IP del iDRAC en Sitios de confianza. Para hacer esto:

1. En Internet Explorer, vaya a **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza**.
2. Compruebe que la opción **Habilitar Modo protegido** no esté seleccionada para la zona de Sitios de confianza. Como alternativa, puede agregar la dirección del iDRAC a sitios en la zona de Intranet. De manera predeterminada, el modo protegido está desactivado para los sitios en la zona de Intranet y en la zona de Sitios de confianza.
3. Haga clic en **Sitios**.
4. En el campo **Agregar este sitio web a la zona**, agregue la dirección del iDRAC y haga clic en **Agregar**.
5. Haga clic en **Cerrar** y luego haga clic en **Aceptar**.
6. Cierre y reinicie el explorador para que la configuración tenga efecto.

Resoluciones de pantalla y velocidades de actualización admitidas

En la Tabla 9-1 se muestra una lista de las resoluciones de pantalla admitidas y las velocidades de actualización correspondientes para una sesión de consola virtual que se ejecuta en el servidor administrado.

Tabla 9-1. Resoluciones de pantalla y velocidades de actualización admitidas

Resolución de pantalla	Velocidad de actualización (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1024 x 768	60, 70, 72, 75, 85
1280 x 1024	60

Configuración de la consola virtual en la interfaz web del iDRAC6

Para configurar la consola virtual en la interfaz web del iDRAC6, realice los pasos siguiente:

1. Haga clic en **Sistema**→ **Consola/Medios**→ **Configuración** para configurar los valores de la consola virtual del iDRAC6.
2. Configure las propiedades de la consola virtual. En la Tabla 9-2 se describen los valores de la consola virtual.
3. Cuando termine, haga clic en **Aplicar** para guardar la nueva configuración.

Tabla 9-2. Propiedades de la configuración de la consola virtual

Propiedad	Descripción
Enabled	Haga clic para activar o desactivar la consola virtual. Si esta opción aparece marcada, indica que la consola virtual está activada. El valor predeterminado es **activada**. **NOTA:** Si la opción **Activada** se marca o se deselecciona una vez después de iniciar la consola virtual, se podrían desconectar todas las sesiones de consola virtual existentes.
N.º máx. de sesiones	Seleccione el número máximo permitido de sesiones de consola virtual, de 1 a 4. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de consola activa. Este campo es de sólo lectura.

Tabla 9-2. Propiedades de la configuración de la consola virtual *(continuación)*

Propiedad	Descripción
Puerto de presencia remota	El número de puerto de red utilizado para conectarse a la opción de teclado/mouse de la consola virtual. 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 una vez después de iniciar la consola virtual, se podrían desconectar todas las sesiones de consola 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 se desactiva una vez después de iniciar la consola virtual, se podrían desconectar todas las sesiones de consola virtual existentes.
Vídeo del servidor local activado	Si está marcado, indica que la salida al monitor de la consola virtual del iDRAC6 se desactiva durante la sesión de consola virtual. Esto garantiza que las tareas que realice usando **Consola virtual** no serán visibles en el monitor local del servidor administrado.
Tipo de complemento	El tipo de complemento que se va a configurar. • **Nativo** (ActiveX para Windows y complemento de Java para Linux): el visor de ActiveX sólo funcionará en Internet Explorer. • **Java**: se iniciará un visor Java.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la consola virtual, ver "Configuración y uso de medios virtuales" en la página 283.

Cómo abrir una sesión de consola virtual

Cuando se abre una sesión de consola virtual, la aplicación Dell Virtual Console Viewer se inicia y el escritorio del sistema remoto aparece en el visor. Con la aplicación Visor de consola virtual, se pueden controlar las funciones de mouse y teclado del sistema remoto desde la estación de administración local.

NOTA: Si la consola virtual se inicia desde una estación de administración Windows Vista, se podrían generar mensajes de reinicio en la consola virtual. Para evitarlo, defina los valores de tiempo de espera adecuados en las siguientes ubicaciones: **Panel de control→ Opciones de energía→ Economizador de energía→ Configuración avanzada→ Disco duro→ Apagar disco duro después de <timeout>** y en **Panel de control→ Opciones de energía→ Alto rendimiento→ Configuración avanzada→ Disco duro→ Apagar disco duro después de <timeout>**.

Para abrir una sesión de consola virtual en la interfaz web, realice los pasos siguientes:

1. Haga clic en **Sistema→ Consola/Medios→ Consola virtual y medios virtuales**.
2. Utilice la información de la Tabla 9-3 para comprobar que hay una sesión de consola virtual disponible.

   Si desea reconfigurar los valores de propiedades que se muestran, ver "Configuración de la consola virtual en la interfaz web del iDRAC6" en la página 229.

Tabla 9-3. Consola virtual

Propiedad	Descripción
Consola virtual activada	Sí/No (seleccionado/no seleccionado)
Cifrado de vídeo activado	Sí/No (seleccionado/no seleccionado)
N.º máx. de sesiones	Muestra el número máximo de sesiones de consola virtual admitidas.
Sesiones activas	Muestra el número actual de sesiones de consola virtual activas.
Vídeo del servidor local activado	Sí = activado; No = desactivado.

Tabla 9-3. Consola virtual *(continuación)*

Propiedad	Descripción
Puerto de presencia remota	El número de puerto de red utilizado para conectarse a la opción de teclado/mouse de la consola virtual. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es 5900.
Tipo de complemento	Muestra el tipo de complemento que se seleccionó en la página **Configuración**. **NOTA:** En las plataformas Windows de 64 bits, el complemento ActiveX de autentificación del iDRAC6 no se instalará correctamente si se ha implementado una versión de 64 bits del "Paquete redistribuible de Microsoft Visual C++ 2005". Para instalar y ejecutar el complemento Active-X correctamente, implemente la versión de 32 bits del Paquete redistribuible de Microsoft Visual C++ 2005 SP1 (x86). Este paquete es necesario para ejecutar la sesión de consola virtual en un explorador Internet Explorer.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la consola virtual, ver "Configuración y uso de medios virtuales" en la página 283.

3 Si hay una sesión de consola virtual disponible, haga clic en **Iniciar consola virtual** la página **Consola virtual y medios virtuales**.

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 los cuadros de mensajes en menos de 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 contenida en la ventana y haga clic en **Sí** para continuar.

La estación de administración se conecta al iDRAC6 y el escritorio del sistema remoto aparece en la aplicación Visor de consola virtual del iDRAC6.

4 Aparecen dos punteros de mouse en la ventana del visor: Uno para el sistema remoto y otro para el sistema local. Puede cambiar a un solo cursor si selecciona la opción **Un solo cursor** en **Herramientas** en el menú de Consola virtual del iDRAC6.

Vista previa de la consola virtual

Antes de iniciar la consola virtual, puede ver una vista previa del estado de la consola virtual en la página **Sistema→ Propiedades→ Resumen del sistema**. La sección **Vista previa de la consola virtual** muestra una imagen del estado de la consola virtual. La imagen se actualiza cada 30 segundos.

NOTA: La imagen de la consola virtual está disponible sólo si se ha activado Consola virtual y si la tarjeta del iDRAC6 Enterprise está presente.

La Tabla 9-4proporciona información acerca de las opciones disponibles.

Tabla 9-4. Opciones de Vista previa de la consola virtual

Opción	Descripción
Iniciar	Haga clic en este vínculo para iniciar la consola virtual. Si sólo está activado Medios virtuales, al hacer clic en este vínculo se inician directamente los medios virtuales. Este vínculo no se muestra si no tiene privilegios para la consola virtual o si tanto la consola virtual como los medios virtuales están desactivados.
Valor	Haga clic en este vínculo para ver o editar los valores de la configuración de la consola virtual en la página **Configuración de la consola/medios**. **NOTA:** Debe configurar los privilegios del iDRAC para poder editar los valores de la configuración de la consola virtual.
Refresh (Actualizar)	Haga clic en este vínculo para actualizar la imagen de la consola virtual que se muestra.

Uso de la consola virtual del iDRAC6 (Video Viewer)

La consola virtual (Video Viewer) del iDRAC6 proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver el escritorio del servidor administrado y controlar las funciones de mouse y teclado desde la estación de administración. Cuando se conecta al sistema remoto, la consola virtual del iDRAC6 se inicia en otra ventana.

NOTA: Debe tener privilegios de administrador para iniciar una consola virtual del iDRAC6 (Video Viewer).

NOTA: Si el servidor remoto está apagado, se visualiza el mensaje **Sin señal**.

NOTA: La barra de título de la consola virtual muestra el nombre DNS o la dirección IP del iDRAC al que se conecta desde la estación de administración. Si el iDRAC no tiene un nombre DNS, se muestra la dirección IP. El formato es: `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

La consola virtual del iDRAC6 proporciona diversos ajustes de control, como por ejemplo, sincronización del mouse, 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 de la interfaz gráfica de usuario **Consola virtual y medios virtuales**.

Cuando inicia una sesión de consola virtual y aparece la consola virtual del iDRAC6, es posible que deba sincronizar los punteros del mouse.

La Tabla 9-5 describe las opciones del menú disponibles en el visor.

Tabla 9-5. Selecciones de la barra de menú del visor

Elemento del menú	Elemento	Descripción
Icono de tachuela	N/D	Haga clic en el icono de tachuela para bloquear la barra de menú de la consola virtual del iDRAC6. Esto evita que la barra de herramientas se oculte automáticamente. **NOTA:** Esto sólo se aplica al visor de ActiveX y no al complemento de Java.

Tabla 9-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Medios virtuales	Iniciar medios virtuales	Muestra la **Sesión de medios virtuales** con una lista de los dispositivos para asignar disponibles en la ventana principal. Para convertir una imagen ISO o IMG en virtual, haga clic en **Agregar** y seleccione el archivo de imagen. El archivo de imagen seleccionado se muestra junto a la lista de dispositivos para asignar disponibles en la ventana principal. Para convertir un dispositivo o una imagen en virtual, marque la opción en la columna **Asignado** de la tabla. El dispositivo o la imagen se asignará al servidor en este punto. Para anular la asignación, deseleccione la casilla. Haga clic en **Detalles** para mostrar el panel en el que se enumeran los dispositivos e imágenes virtuales. También se muestra la actividad de lectura/escritura de cada dispositivo o imagen.
Archivo	Capturar en archivo	Captura la pantalla actual del sistema remoto en un archivo **.bmp** en Windows o en un archivo **.png** en Linux. Aparece un cuadro de diálogo que permite guardar el archivo en un lugar determinado. **NOTA:** El formato de archivo **.bmp** en Windows o el formato de archivo **.png** en Linux sólo se aplican al complemento nativo. El complemento de Java sólo admite los formatos de archivo **.jpg** y **.jpeg**.
	Salir	Cuando haya terminado de usar la consola y se haya desconectado (mediante el procedimiento de desconexión del sistema remoto), seleccione **Salir** desde el menú **Archivo** para cerrar la ventana **Consola virtual del iDRAC6**.

Tabla 9-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Ver	**Refresh (Actualizar)**	Actualiza la vista de la consola virtual de vídeo. La consola virtual solicita al servidor un marco de vídeo de referencia.
	Pantalla completa/ En ventanas	Vista de la consola virtual de vídeo en modo de pantalla completa. Para salir del modo de pantalla completa, haga clic en **En ventanas**.
	Ajustar	Cambia el tamaño de la ventana de la consola virtual de vídeo al tamaño mínimo requerido para mostrar el vídeo del servidor. Este elemento del menú no está disponible en el modo de pantalla completa.

Tabla 9-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Macros	• Alt+Ctrl+Supr • Alt+Tab • Alt+Esc • Ctrl+Esc • Alt+Espacio • Alt+Intro • Alt+Guión • Alt+F4 • ImprPant • Alt+ImprPant • F1 • Pause • Lengüeta • Ctrl+Intro • PetSis • Alt+MayúsIzq+MayúsDer+Esc • Ctrl+Alt+Retroceso • Alt+F? (Donde F? representa las teclas F1-F12) • Ctrl+Alt+F? (Donde F? representa las teclas F1-F12)	Al seleccionar una macro o presionar la tecla aceleradora especificada para la macro, la acción se ejecuta en el sistema remoto.

Tabla 9-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Herramientas	Opciones de la sesión	La ventana Opciones de la sesión proporciona ajustes de control adicionales al visor de la sesión. Esta ventana tiene las fichas **General** y **Mouse**. Se puede controlar el **modo de paso a través de teclado** en la ficha General. Seleccione **Pasar todas las pulsaciones de teclas al destino** para pasar las pulsaciones de teclas de la estación de administración al sistema remoto. La ficha Mouse contiene dos secciones: **Cursor sencillo** y **Aceleración del mouse**. La función **Cursor sencillo** se proporciona para compensar los problemas de alineación del mouse en algunos sistemas operativos remotos. Una vez que el visor entra al modo **Cursor sencillo**, el puntero del mouse queda atrapado dentro de la ventana del visor. Presione la tecla de terminación para salir de esta modalidad. Utilice este control para seleccionar la tecla que saldrá del modo de cursor sencillo. La **Aceleración del mouse** optimiza el funcionamiento del mouse en función del sistema operativo.
	Cursor sencillo	Activa el modo de cursor sencillo en el visor. En este modo, el cursor del cliente se oculta de la vista, de manera que sólo queda visible el cursor del servidor. El cursor del cliente también queda atrapado en el marco del visor. El usuario no podrá utilizar el cursor fuera de la ventana del visor hasta que presione la **Tecla de terminación** que se especifica en la ficha **Opciones de sesión: Mouse**.
	Estadísticas	Esta opción del menú abre un cuadro de diálogo que muestra estadísticas de rendimiento del visor. Los valores que se muestran son: • Velocidad de imagen • Ancho de banda • Compresión • Velocidad de paquetes

Tabla 9-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Alimentación	Encender el sistema	Enciende el sistema.
	Apagar el sistema	Apaga el sistema.
	Apagado ordenado	Apaga el sistema. **NOTA:** Compruebe que la opción de apagado está configurada para el sistema operativo antes de realizar un apagado ordenado utilizando esta opción. Si utiliza esta opción sin configurarla en el sistema operativo, se reinicia el sistema administrado en lugar de realizar una operación de apagado.
	Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo.
	Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)	Apaga y luego reinicia el sistema.
Help (Ayuda)	Contenido e índice	Proporciona instrucciones para ver la ayuda en línea.
	Acerca de la consola virtual del iDRAC6	Muestra la versión de **Consola virtual del iDRAC6**.

Desactivación o activación del vídeo del servidor local

Se puede configurar el iDRAC6 para rechazar conexiones de la consola virtual del iDRAC6 por medio de la interfaz web del iDRAC6.

Si desea asegurarse de tener acceso exclusivo a la consola del servidor administrado, debe desactivar la consola local *y* volver a configurar el **Máx. de sesiones** a `1` en la página **Configuración de la consola virtual**.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, el monitor, el teclado y el mouse que están conectados a la consola virtual del iDRAC6 permanecen activados.

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.
2. Haga clic en **Sistema→ Consola/Medios→ Configuración**.

3 Para desactivar (apagar) el vídeo local en el servidor, desmarque la casilla **Vídeo del servidor local activado** en la página **Configuración**, y luego haga clic en **Aplicar**. El valor predeterminado es Apagado.

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 **Vídeo del servidor local activado** en la página **Configuración**, y luego haga clic en **Aplicar**.

Inicio de la consola virtual y de los medios virtuales de manera remota

Se puede iniciar la consola virtual o los medios virtuales introduciendo un solo URL en un explorador admitido, en lugar de iniciarlo desde la interfaz gráfica de usuario web del iDRAC6. Dependiendo de la configuración del sistema, se realiza el proceso de autentificación manual (página de inicio de sesión) o se dirige automáticamente al visor de la consola virtual o de los medios virtuales.

Si el inicio de sesión único ya está configurado en el sistema, no podrá utilizar el formato de URL para iniciar la consola virtual o los medios virtuales.

Puede iniciar la consola virtual con una cuenta de usuario creada localmente en iDRAC6, LDAP y Active Directory.

NOTA: Internet Explorer admite el inicio de sesión local, con Active Directory (AD), tarjeta inteligente (SC) e inicio de sesión único (SSO). Firefox admite sólo el inicio de sesión local, AD e inicio de sesión único en sistemas operativos basados en Windows. No admite el inicio de sesión SC.

Inicio de la consola mediante el formato de URL

Si introduce el `vínculo <IP>/console` en un explorador, inicie sesión siguiendo el procedimiento de inicio de sesión manual normal según la configuración de inicio de sesión. Si el inicio de sesión se realiza satisfactoriamente, la consola virtual o los medios virtuales se inician. De lo contrario, se redirige al usuario a la página de inicio de la interfaz gráfica de usuario del iDRAC6.

La sesión de la interfaz gráfica web del iDRAC se muestra en segundo plano en la página de vKVM.

Puede iniciar tan sólo una sesión de la consola virtual a la vez.

Si tiene activados los privilegios de sólo lectura utilice el formato de URL para iniciar sólo la página Consola virtual y no la página Medios virtuales.

Si la consola virtual está desactivada en el iDRAC6, el usuario o el administrador todavía pueden iniciar los medios virtuales, si tienen privilegios suficientes. Para obtener más información sobre privilegios suficientes, ver "Inicio de la consola virtual y de los medios virtuales de manera remota" en la página 240.

Situaciones de error habituales

La Tabla 9-6 muestra una lista de las situaciones de error habituales, los motivos de los errores y el comportamiento del iDRAC6.

Tabla 9-6. Situaciones de error

Situaciones de error	Motivo	Comportamiento
Falló el inicio de sesión	Ingresó un nombre de usuario no válido o una contraseña incorrecta.	Se presenta el mismo comportamiento cuando se especifica *https://<IP>* y el inicio de sesión falla.
La tarjeta de iDRAC6 Enterprise no está presente	La tarjeta de iDRAC6 Enterprise no está presente. Por lo tanto, la función de consola virtual/medios virtuales no está disponible.	El visor de la consola virtual de iDRAC6 no se ha iniciado. Se redirige al usuario a la página de inicio de la interfaz gráfica de usuario del iDRAC6.
Privilegios insuficientes	No cuenta con privilegios de consola virtual y medios virtuales.	El visor de la consola virtual de iDRAC6 no se inicia y el usuario es redirigido a la página de la interfaz gráfica de usuario de configuración de la consola o los medios.
Consola virtual desactivada	La consola virtual está desactivada en su sistema.	El visor de la consola virtual de iDRAC6 no se inicia y el usuario es redirigido a la página de la interfaz gráfica de usuario de configuración de la consola o los medios.
Se detectaron parámetros de URL desconocidos	El URL introducido incluye parámetros no definidos.	Aparece el mensaje No se encontró la página (404).

Preguntas frecuentes sobre la consola virtual

La Tabla 9-7 contiene las preguntas y respuestas frecuentes.

Tabla 9-7. Uso de la consola virtual: preguntas frecuentes

Pregunta	Respuesta
La consola virtual no cierra la sesión cuando se desconecta la interfaz gráfica de usuario web fuera de banda.	Las sesiones de la consola virtual y los medios virtuales permanecen activas incluso cuando la sesión de web se desconecta. Cierre las aplicaciones del visor de medios virtuales y de la consola virtual para desconectarse de la sesión correspondiente.
¿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?	Para que el usuario local tenga 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 mouse 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.

Tabla 9-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿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 la consola virtual** 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 la consola virtual.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024. Intente también utilizar las barras de desplazamiento en el cliente de la consola virtual del iDRAC6.
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 el mouse no se sincroniza en la consola de texto de Linux (en Dell Unified Server Configurator (USC), Dell Lifecycle Controller o en Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)?	La consola virtual requiere el controlador de mouse USB, pero el controlador de mouse USB sólo está disponible en el sistema operativo X-Window.
Aún tengo problemas con la sincronización del mouse.	Compruebe que está seleccionado el mouse adecuado al sistema operativo antes de iniciar una sesión de consola virtual. Compruebe que la opción **Un solo cursor** en **Herramientas**, en el menú de la consola virtual de iDRAC6, esté seleccionada en el cliente de la consola virtual de iDRAC6. La opción predeterminada es el modo de dos cursores.

Tabla 9-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Por qué no puedo usar un teclado o un mouse mientras instalo un sistema operativo Microsoft de manera remota mediante la consola virtual del iDRAC6?	Cuando se instala de manera remota un sistema operativo Microsoft admitido en un sistema con la consola virtual activada en el BIOS, aparece un mensaje de conexión de EMS que pide que se seleccione **Aceptar** para poder continuar. No se puede usar el mouse para seleccionar **Aceptar** de manera remota. Se debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la consola virtual en el BIOS. Microsoft genera este mensaje para avisar al usuario que la consola virtual está activada. Para asegurar que este mensaje no aparezca, siempre desactive la consola virtual 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 estado de Bloq Num en el servidor remoto?	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 configuración del servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Num en la estación de administración.
¿Por qué aparecen varias ventanas del visor de sesión cuándo establezco una sesión de consola virtual desde el host local?	Está configurando una sesión de consola virtual desde el sistema local. Esto no se permite.
Si estoy ejecutando una sesión de consola virtual y un usuario local accede al servidor administrado, ¿recibiré un mensaje de advertencia?	No. Si un usuario local accede al sistema, ambos tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de consola virtual?	Se recomienda tener una conexión de 5 MB/s para obtener un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.

Tabla 9-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la consola virtual?	La estación de administración requiere un procesador Intel Pentium III a 500 MHz con un mínimo de 256 MB de RAM.
¿Por qué aparece el mensaje **Sin señal** dentro del visor de vídeo de la consola virtual del iDRAC6?	Es posible que el mensaje aparezca porque el complemento de la consola virtual del iDRAC6 no está recibiendo el vídeo del escritorio del servidor remoto. Generalmente, este comportamiento suele ocurrir cuando el servidor remoto está apagado. Ocasionalmente, el mensaje puede aparecer debido a una falla en la recepción del vídeo del escritorio del servidor remoto.
¿Por qué aparece el mensaje **Fuera de rango** dentro del visor de vídeo de la consola virtual del iDRAC6?	Es posible que este mensaje aparezca porque un parámetro necesario para capturar vídeo esté fuera del rango en el cual el iDRAC6 puede capturar vídeo. Parámetros tales como la resolución de pantalla o la frecuencia de actualización cuando son muy elevados provocan una condición de fuera de rango. Por lo general, el rango máximo de parámetros está definido por limitaciones físicas como el tamaño de la memoria de vídeo o el ancho de banda.

10

Uso de la interfaz WS-MAN

Servicios web para administración (WS–MAN) es un protocolo basado en el protocolo simple de acceso a objetos (SOAP), utilizado en la administración de sistemas. WS–MAN proporciona un protocolo con capacidad interoperativa para que los dispositivos puedan compartir e intercambiar datos a través de redes. El iDRAC6 utiliza WS–MAN para transmitir información de administración basada en el modelo común de información (CIM) del grupo de trabajo de administración distribuida (DMTF); la información del CIM define la semántica y los tipos de información que pueden manipularse en un sistema administrado. Las interfaces incorporadas por Dell para la administración de plataformas de servidores están organizadas en perfiles, en los que cada perfil define las interfaces específicas para cada dominio de administración o área de funcionalidad en particular. Además, Dell ha definido diversas extensiones de modelo y perfil que ofrecen interfaces para otras capacidades.

Los datos que se encuentran disponibles a través de WS-MAN son provistos por la interfaz de instrumentación del iDRAC6 asignada a los siguientes perfiles DMTF y de extensión de Dell:

Perfiles CIM admitidos

Tabla 10-1. DMTF estándar

DMTF estándar
1 Servidor básico Define las clases de CIM para representar al servidor host.
2 Procesador de servicio: Contiene la definición de las clases de CIM para representar al iDRAC6.
3 Propiedad física: Define las clases de CIM para representar el aspecto físico de los elementos administrados. El iDRAC6 utiliza este perfil para representar la información de FRU del servidor host.

Tabla 10-1. DMTF estándar *(continuación)*

DMTF estándar
4 Admin de dominios SM-CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del 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 de 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 alimentación, como los límites máximo y mínimo de consumo de alimentación.
7 Servicio CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
8 Interfaz IP
9 Cliente DHCP
10 Cliente DNS
11 Puerto Ethernet Los perfiles anteriores definen las clases de CIM para representar pilas de redes El iDRAC6 usa estos perfiles para representar la configuración del NIC 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 sucesos 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.

Tabla 10-1. DMTF estándar *(continuación)*

DMTF estándar
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 del CLP. El iDRAC6 usa este perfil para su propia implementación del 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 Métricas básicas Define las clases de CIM para representar las métricas. El iDRAC6 usa este perfil para representar las métricas del servidor host para describir el consumo de alimentación, como los límites máximo y mínimo de consumo de alimentación.
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.

Tabla 10-1. DMTF estándar *(continuación)*

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 de banda lateral del NIC para el NIC 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.
5 Implementación del sistema operativo Dell Define las clases de extensión de CIM y Dell para representar la configuración de las funciones de implementación de sistema operativo. Amplía la función de administración de hacer referencia a los perfiles al sumar la compatibilidad con actividades de implementación de sistema operativo manipulando las funciones de ese tipo de implementación que ofrece el procesador de servicio.
6 Control de trabajos de Dell Define las clases de extensiones de CIM y Dell para administrar trabajos de configuración.
7 Perfil de administración de LC de Dell Define las clases de extensiones de CIM y Dell para configurar los atributos de Dell Lifecycle Controller, como el descubrimiento automático. Este perfil también activa la administración del reemplazo de piezas, del reemplazo de la placa madre, la exportación e importación del perfil de sistema, el inicio desde un recurso compartido de red y la administración del certificado de cifrado.
8 Almacenamiento persistente de Dell Define las clases de extensiones de CIM y Dell para administrar las particiones en la tarjeta vFlash SD de las plataformas Dell.
9 NIC simple de Dell Define las clases de extensiones de CIM y Dell para representar la configuración de los controladores de red de NIC.

Tabla 10-1. DMTF estándar *(continuación)*

Extensiones de Dell
10 Perfil de administración del BIOS y del inicio de Dell Define las clases de extensiones de CIM y Dell para representar los atributos del BIOS de Dell y para configurar la secuencia de inicio del host.
11 Perfil de RAID de Dell Define las clases de extensiones de CIM y Dell para representar la configuración del almacenamiento de RAID del host.
12 Perfil de suministro de energía de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del suministro de energía del host.
13 Perfil de la tarjeta del iDRAC de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del iDRAC6. Este perfil también proporciona una representación y métodos para configurar atributos y cuentas de usuarios iDRAC.
14 Perfil de ventiladores de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del ventilador del host.
15 Perfil de memoria de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del DIMM del host.
16 Perfil del CPU de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del CPU del host.
17 Perfil de información del sistema de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario de la plataforma del host.
18 Perfil del dispositivo PCI de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario del PCI del host.
19 Perfil de vídeo de Dell Define las clases de extensiones de CIM y Dell para representar la información de inventario de la tarjeta de vídeo del host.

La implementación de WS-MAN del iDRAC6 utiliza SSL en el puerto 443 para garantizar la seguridad de transporte y admite autentificación básica y de resumen. Las interfaces de los servicios web se pueden utilizar mediante el aprovechamiento de la infraestructura del cliente, como la interfaz de línea de comandos WinRM y Powershell de Windows, las utilidades de código abierto como WSMANCLI y entornos de programación de aplicaciones como Microsoft .NET.

Para obtener más información sobre los servicios remotos de Dell Lifecycle Controller, consulte los documentos siguientes:

- Guía del usuario
- Notas de la versión
- Lista de mensajes de error y solución de problemas

Para acceder a estos documentos:

1. Vaya a **dell.com/support/manuals**.
2. Haga clic en **Software→ Administración del sistema→ Dell Unified Server Configurator and Lifecycle Controller**.
3. Haga clic en la versión relevante para ver todos los documentos para una versión concreta.

Para acceder a guías, documentos de perfil, muestras de códigos, documentos técnicos y otra información útil de la interfaz de servicios web (Windows y Linux), vaya a **OpenManage Systems Management→ Lifecycle Controller** en **delltechcenter.com**.

Para obtener más información, consulte lo siguiente:

- Sitio web de DMTF en **dmtf.org/standards/profiles/**
- Notas de publicación o archivo léame de WS–MAN.

11

Uso de la interfaz de línea de comandos SM-CLP del iDRAC6

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 de arquitectura de administración de sistemas para hardware de servidor (SMASH) y las especificaciones de SM-CLP. Para obtener más información sobre estas especificaciones, visite el sitio web de DMTF en **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

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. El SM-CLP del iDRAC6 admite todos los perfiles descritos en la Tabla 10-1.

Las siguientes secciones proporcionan una descripción de la función SM-CLP que se aloja en el iDRAC6.

Funciones de SM-CLP

El SM-CLP promueve el concepto de verbos y destinos para proporcionar 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.

Vea el siguiente ejemplo de la sintaxis de la línea de comandos de SM-CLP.

```
<verb> [<options>] [<target>] [<properties>]
```

Durante una sesión típica de SM-CLP, puede realizar operaciones mediante los verbos que se mencionan en la Tabla 11-1.

Tabla 11-1. Verbos de interfaz de línea de comandos 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

SSH (o Telnet) con el iDRAC6 mediante las credenciales correctas.

Se muestra la petición SMCLP (/admin1->).

Destinos de SM-CLP

Tabla 11-2 contiene una lista de los destinos que se proporcionan por medio de SM-CLP para sustentar las operaciones que se describen en la Tabla 11-1 anteriormente.

Tabla 11-2. 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 recopilaciones de registro
admin1/system1/logs1/log1	Entrada de registro de sucesos del sistema (SEL)
admin1/system1/logs1/log1/record*	Una entrada individual del registro de sucesos 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

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
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/capabilitie s1	Recopilación SMASH de las capacidades del procesador de servicio
admin1/system1/sp1/capabilitie s1/clpcap1	Capacidades del servicio CLP
admin1/system1/sp1/capabilitie s1/pwrmgtcap1	Capacidades del servicio de administración del estado de la alimentación en el sistema
admin1/system1/sp1/capabilitie s1/ipcap1	Capacidades de la interfaz IP
admin1/system1/sp1/capabilitie s1/dhcpcap1	Capacidades del cliente DHCP
admin1/system1/sp1/capabilitie s1/NetPortCfgcap1	Capacidades de configuración del puerto de red
admin1/system1/sp1/capabilitie s1/usbredirectcap1	SAP de redirección de USB de capacidades de medios virtuales
admin1/system1/sp1/capabilitie s1/vmsapcap1	Capacidades SAP de medios virtuales

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
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 autentificación 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*	Anotación 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

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
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/NetPortCfgs vc1	Servicio de configuración del puerto de red
admin1/system1/sp1/lanendpt1	Punto final de la LAN
admin1/system1/sp1/ lanendpt1/enetport1	Puerto Ethernet

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
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 autentificación 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) locales
admin1/system1/sp1/rolesvc1/ Role1-16	Función local

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
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 sobre 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

Tabla 11-2. Destinos de SM-CLP *(continuación)*

Destino	Definiciones
/admin1/system1/sp1/metricsvc1 /cumampamd1	Definición métrica de concentración acumulativa de amperios
/admin1/system1/sp1/metricsvc1 /cumampamd1/cumampamv1	Valor métrico de concentración acumulativa de amperios
/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

12

Instalación del sistema operativo mediante VMCLI

La utilidad de interfaz de línea de comandos de medios virtuales (VMCLI) es una interfaz de línea de comandos que proporciona 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, es posible instalar el sistema operativo en varios sistemas remotos de una red.

Esta sección contiene información acerca de cómo integrar la utilidad VMCLI en una 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 del sistema remoto

El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Un recurso compartido de red debe tener los siguientes componentes:

- Los archivos del sistema operativo
- Los archivos controladores requeridos
- 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 de la industria.

Creación de un archivo de imagen de inicio

Antes de implementar el archivo de imagen en los sistemas remotos, compruebe que un sistema admitido pueda 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 proporcionan información específica para la creación de archivos de imagen para sistemas Linux y Microsoft Windows.

Creación de un archivo de imagen para sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen de inicio para el sistema Linux.

Para ejecutar la utilidad, abra un símbolo del sistema 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 sistemas Windows

Al momento de elegir una utilidad de replicador de datos para crear 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 implementación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que pueda acceder desde la estación de administración.
2. Copie los archivos del sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen de inicio preconfigurado para implementar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen de inicio preconfigurado para implementación, prepárelo. Incluya los programas o secuencias de comandos que se van a utilizar en los procedimientos de implementación 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 estándar 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 implementación

4 Realice uno de los procedimientos siguientes:

- Integre **IPMItool** y VMCLI en la aplicación existente de implementación del sistema operativo. Use la secuencia de comandos **vm6deploy** de ejemplo como guía para usar la utilidad.
- Utilice la secuencia de comandos **vm6deploy** existente para implementar el sistema operativo.

Implementación del sistema operativo

Use la utilidad VMCLI y la secuencia de comandos **vm6deploy** que se incluye con la utilidad para implementar 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 implementar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para implementar el sistema operativo en los sistemas remotos de destino.

1 Haga una lista de las direcciones IPv4 o IPv6 del iDRAC6 de los sistemas remotos que serán implementados en el archivo de texto **ip.txt**, una dirección IPv4 o IPv6 por línea.

2 Inserte un CD o DVD de inicio 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 la línea de comandos:

```
vm6deploy -r ip.txt -u <usuario_del_iDRAC> -p
<contraseña_de_usuario_de_iDRAC> -c {<imagen_iso9660> |
<ruta_de_acceso>} -f {<floppy-device> o <floppy-image>}
```

donde:

- *<usuario_del_idrac>* es el nombre de usuario del iDRAC6, por ejemplo, **root**
- *<contraseña_de_usuario_de_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
- -f {*<dispositivo_de_disco_flexible>*} es la ruta de acceso al dispositivo que contiene el CD, DVD o disco flexible de instalación del sistema operativo
- *<imagen_de_disco_flexible>* es la ruta de acceso a una imagen de disco flexible válida

La secuencia de comandos **vm6deploy** pasa las opciones de línea de comandos a la utilidad **VMCLI**. Ver "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 lee las direcciones IPv4 o IPv6 del iDRAC6 del archivo especificado y ejecuta la utilidad **VMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, debe ser entonces 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 proporciona las funciones de medios virtuales desde la estación de administración al iDRAC6.

La utilidad VMCLI proporciona las siguientes funciones:

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 coherentes 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.

PRECAUCIÓN: Se recomienda utilizar la opción "-i" del indicador interactivo al iniciar la utilidad de línea de comandos VMCLI. Esto garantiza una seguridad más estricta gracias a que el nombre de usuario y la contraseña se mantienen privados porque, en muchos sistemas operativos Windows y Linux, el nombre de usuario y la contraseña están visibles cuando otros usuarios examinan los procesos.

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 proporciona un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos de 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* (Documentación y herramientas de Dell Systems Management) 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* (Documentación y herramientas de Dell Systems Management) en la unidad correspondiente del sistema y siga las instrucciones que aparecen en pantalla.

El DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) contiene los productos de software de administración de sistemas más recientes, incluso la administración de almacenamiento, el servicio de acceso remoto y la utilidad IPMItool. Este DVD también contiene archivos léame con la más reciente información de producto del software de administración de sistemas.

Además, el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) incluye **vm6deploy**: una secuencia de comandos de ejemplo que ilustra el uso de las utilidades VMCLI e IPMItool para implementar 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, debe 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. Ver “Parámetros de VMCLI” en la página 269 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_de_iDRAC[:puerto_SSL_de_iDRAC]>`

Este parámetro proporciona la dirección IPv4 o IPv6 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 o IPv6 que no son válidos, aparece un mensaje de error y el comando termina.

<dirección_IP_de_iDRAC> es una dirección IPv4 o IPv6 válida y exclusiva 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 utiliza 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 <usuario_de_iDRAC>`

Este parámetro proporciona el nombre de usuario del iDRAC6 que ejecutará los medios virtuales.

El *<usuario_de_iDRAC>* debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales del iDRAC6

Si la autentificación del iDRAC6 falla, aparece un mensaje de error y el comando termina.

Contraseña de usuario del iDRAC6

`-p <contraseña_de_usuario_del_iDRAC>`

Este parámetro proporciona la contraseña para el usuario del iDRAC6 especificado.

Si la autentificación del iDRAC6 falla, aparece un mensaje de error y se termina el comando.

Archivo de imagen o dispositivo de disco/disco flexible

`-f {<floppy-device> o <floppy-image>}` y/o

`-c {<CD-DVD-device> o <CD-DVD-image>}`

donde <floppy-device> o `<CD-DVD-device>` es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido (para sistemas Linux) e `<floppy-image> o <CD-DVD-image>` es el nombre de archivo 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 disco flexible.

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 disco flexible que no desea que se sobrescriba.

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`-f /dev/sdb4 # 4ª partición en el dispositivo /dev/sdb` (sistema Linux)

NOTA: Red Hat Enterprise Linux versión 4 no admite varios LUN. Sin embargo, el núcleo admite esta función. Permita que Red Hat Enterprise Linux versión 4 reconozca un dispositivo SCSI con varios números LUN por medio de 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 núcleo; 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 núcleo, cuyo nombre determinó en el paso 2:

```
mkinitrd /boot/initrd-'uname -r'.img 'uname -r'
```

4 Reinicie 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 discos flexibles. Si se detecta un valor no válido, aparece un mensaje de error y el comando termina.

Archivo de imagen o dispositivo de CD/DVD

`-c {<device-name> | <image-file>}`

donde <*device-name*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas Linux) y <*image-file*> es el nombre y la ruta de acceso de un archivo de imagen ISO-9660 válido.

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 medios CD/DVD. Si se detecta un valor no válido, aparece un mensaje de error y el comando termina.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, salvo que sólo se tengan opciones de interruptor. De lo contrario, aparece un mensaje de error y el comando termina y genera 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 conmutadores, el comando termina 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 termina sin errores.

Datos cifrados

`-e`

Cuando se incluye este parámetro en la línea de comandos, VMCLI usa un *canal cifrado con SSL* para transferir datos entre la estación de administración y el iDRAC6 del sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifra.

NOTA: El uso de esta opción no cambia el estado de cifrado de los medios virtuales mostrados 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: redirige los mensajes impresos de la utilidad hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre de 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 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.

Esta 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 bloquea hasta que el programa VMCLI se termina). Cuando se inician varias instancias de VMCLI de esta manera, y una o varias de las instancias de comando se terminan manualmente, utilice las instalaciones específicas del sistema operativo para enumerar y terminar procesos.

Códigos de retorno de VMCLI

Cuando se presentan errores, se envían mensajes de texto en inglés a la salida estándar de errores.

13

Configuración de la interfaz de administración de plataforma inteligente

Esta sección proporciona información sobre cómo configurar y usar la interfaz IPMI del iDRAC6 La interfaz incluye lo siguiente:

- IPMI en la LAN
- IPMI en 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 de usuario del iDRAC6 de su explorador
- Una utilidad de código fuente 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 *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage) en **support.dell.com\manuals.**

Para obtener más información sobre cómo usar RACADM, ver "Uso de RACADM de manera remota" en la página 120.

Configuración de IPMI mediante la interfaz web

Para obtener más información, ver "Configuración de IPMI por medio de la interfaz web" en la página 65.

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. Ver "Uso de RACADM de manera remota" en la página 120.
2. Configure la IPMI en la LAN.

   Abra un símbolo del sistema, escriba el comando siguiente y presione <Intro>:

   ```
   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 de IPMI 2.0.

   a. Actualice los privilegios de canal de IPMI.

   En el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

   ```
   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 del 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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 de IPMI 2.0.

En el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <identificación> 2
```

donde *<id>* 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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

b Establezca la velocidad en baudios de la conexión serie de IPMI.

Abra un símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

d Establezca el nivel mínimo de privilegios de canal de conexión serie de IPMI.

En el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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 autoprueba de encendido, o POST, presione <F2> para entrar al programa de configuración del BIOS.
- Haga clic en **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.

La configuración de IPMI se ha completado.

Si la conexión serie de IPMI está en modo de terminal, puede configurar los siguientes valores adicionales por medio de los comandos **racadm config cfgIpmiSerial**:

- Control de eliminación
- Control del eco
- Edición de línea
- Nuevas secuencias de línea
- Entrada de nuevas secuencias de 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 que provienen 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 el indicador de comandos, escriba:

   ```
   racadm config -g cfgSerial -o
   cfgSerialConsoleEnable 0
   ```

2 Active el modo IPMI adecuado.

Por ejemplo, en el símbolo del sistema, escriba:

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode <0 ó 1>
```

Para obtener más información, consulte las definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6 de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Configuración de la comunicación en serie en la LAN mediante la interfaz web

Para obtener más información, ver "Configuración de IPMI por medio de la interfaz web" en la página 65.

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 *Dell OpenManage Baseboard Management Controller Utilities User's Guide* (Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage) en **support.dell.com\manuals**.

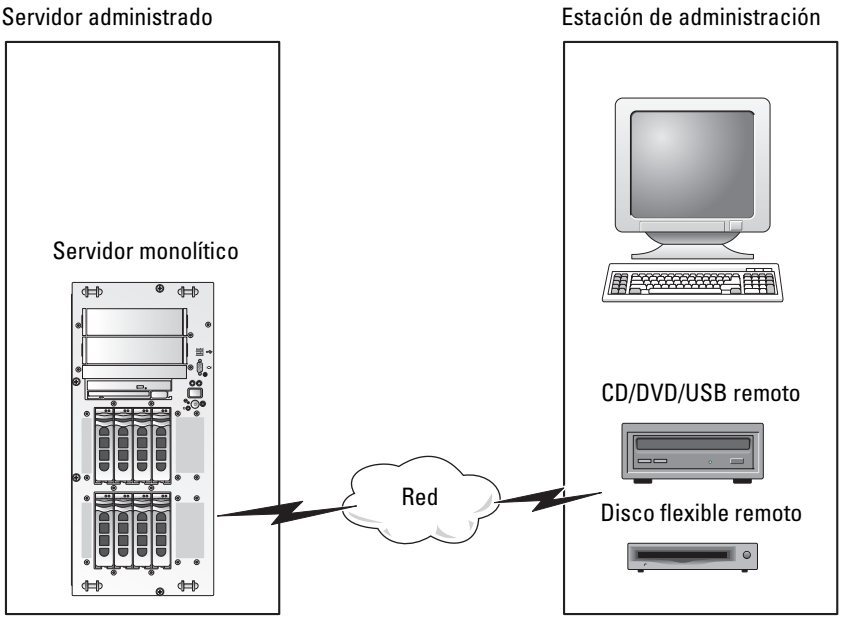
14

Configuración y uso de medios virtuales

Descripción general

La función **Medios virtuales**, a la que se puede acceder mediante el visor de la consola virtual, proporciona al servidor administrado acceso a medios conectados a un sistema remoto en la red. La Ilustración 14-1 muestra la arquitectura general de los **medios virtuales**.

Ilustración 14-1. 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 unidades CD/DVD y discos virtuales.

NOTA: Los **medios virtuales** requieren un ancho de banda de red mínimo disponible de 128 Kbps.

Los **medios virtuales** definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: un dispositivo de disco flexible y otro 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 disco flexible 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 del sistema administrado aparecen como dos unidades sin que los medios se encuentren instalados en las unidades.

La Tabla 14-1 enumera las conexiones compatibles de unidades ópticas virtuales y de discos flexibles virtuales.

NOTA: Si cambia los **medios virtuales** mientras están conectados, podría detenerse la secuencia de inicio del sistema.

Tabla 14-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 con disco flexible de 1,44	Unidad combinada de CD-ROM, DVD, CD-RW, con medios CD-ROM
Unidad de disco flexible USB con un disco flexible de 1,44	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44	Unidad de CD-ROM USB con medios CD-ROM
Disco extraíble USB	

Estación de administración basada en Windows

Para ejecutar la función **Medios virtuales** en una estación de administración que ejecuta el sistema operativo Microsoft Windows, instale una versión admitida de Internet Explorer o Firefox con Java Runtime Environment (JRE).

Estación de administración basada en Linux

Para ejecutar la función Medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Firefox.

Se requiere Java Runtime Environment (JRE) de 32 bits para ejecutar el complemento de consola virtual. Puede descargar JRE desde el sitio **java.sun.com**.

PRECAUCIÓN: Para iniciar Medios virtuales satisfactoriamente, asegúrese de haber instalado una versión de JRE de 32 o de 64 bits en un sistema operativo de 64 bits, o una versión de JRE de 32 bits en un sistema operativo de 32 bits. El iDRAC6 *no* admite las versiones de ActiveX de 64 bits. Asimismo, para Linux se debe tener instalado el paquete "compat-libstdc++-33-3.2.3-61" relacionado a fin de poder ejecutar los medios virtuales. En Windows, el paquete puede venir incluido en el paquete de .NET Framework.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Sistema→ ficha Consola/Medios→ Configuración→ Medios virtuales** para configurar los valores de los medios virtuales.

   La Tabla 14-2 describe los valores de configuración de los **medios virtuales**.
3. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.

Tabla 14-2. Propiedades de configuración de los medios virtuales

Atributo	Valor
Estado	**Conectar**: conecta inmediatamente los **medios virtuales** al servidor. **Desconectar**: desconecta inmediatamente los **medios virtuales** del servidor. **Conectar automáticamente**: conecta los **medios virtuales** al servidor solamente cuando se inicia una sesión de medios virtuales.

Tabla 14-2. Propiedades de configuración de los medios virtuales *(continuación)*

Atributo	Valor
N.º 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 marcación 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 disco flexible	Indica si los **medios virtuales** aparecen como unidad de disco flexible o como memoria USB en el servidor. Si se selecciona **Emulación de disco flexible**, el dispositivo **medios virtuales** aparece como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB. **NOTA:** En ciertos entornos de Windows Vista y Red Hat, es posible que no pueda convertir en virtual un USB con **Emulación de disco flexible** activada.
Estado de conexión	**Conectado**: hay una sesión de medios virtuales en progreso actualmente. **No conectado**: no hay una sesión de medios virtuales en progreso actualmente.
Activar el inicio único	Seleccione esta casilla para activar la opción **Iniciar una vez**. Utilice este atributo para iniciar el sistema desde los medios virtuales. Durante el siguiente inicio, seleccione el dispositivo de inicio en el menú de inicio del BIOS. Esta opción desconecta automáticamente los dispositivos de **medios virtuales** después de que el sistema se inicia una vez.

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 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 disco flexible virtual:

   ```
   cat /proc/scsi/scsi
   ```

NOTA: A través de los medios virtuales, puede virtualizar una sola unidad de disco flexible /unidad/imagen/memoria USB y una unidad óptica de su estación de administración para que esté disponible como unidad (virtual) en el servidor administrado.

Configuraciones admitidas de medios virtuales

Puede activar los medios virtuales para una unidad de disco flexible y una unidad de discos ópticos. Sólo se puede virtualizar una unidad a la vez por cada tipo de medio.

Las unidades de disco flexible que se admiten incluyen una imagen de disco flexible o una unidad de disco flexible 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 web compatible en la estación de administración.

2 Inicie la interfaz web del iDRAC6. Para obtener más información, ver "Acceso a la interfaz web" en la página 50.

3 Seleccione **Sistema→ Consola/Medios→ Consola virtual** y Medios virtuales.

4 Aparece la página **Consola virtual y Medios virtuales**. Si desea cambiar los valores de cualquiera de los atributos mostrados, ver "Configuración de los medios virtuales" en la página 285.

NOTA: Es posible que aparezca **Archivo de imagen de disco flexible** bajo **Unidad de disco flexible** (si se aplica), pues este dispositivo se puede virtualizar como un disco virtual. Puede seleccionar una unidad óptica y una unidad de disco flexible/memoria USB al mismo tiempo para virtualizar.

NOTA: Las letras de unidad de los dispositivos virtuales del servidor administrado no coinciden con las letras de las unidades físicas de la estación de administración.

NOTA: Es posible que los **medios virtuales** no funcionen correctamente en los clientes con sistema operativo Windows configurados con seguridad mejorada en Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador del sistema.

5 Haga clic en **Iniciar Consola virtual**.

NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo pregunta 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 **Consola virtual de iDRAC6** se inicia en otra ventana.

6 Haga clic en **Medios virtuales→ Iniciar Medios virtuales**.

Aparece el asistente de **Sesión de medios virtuales**.

NOTA: No cierre este asistente a menos que desee terminar la sesión de medios virtuales.

7 Si hay algún medio conectado, debe desconectarlo antes de conectar otro medio diferente. Deseleccione la casilla a la izquierda del medio que desea desconectar.

8 Seleccione los tipos de medio que desea conectar.

Si desea conectar una imagen de disco flexible 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 diríjase al directorio donde se encuentra la imagen.

Los medios están conectados y la ventana de **estado** se actualiza.

Desconexión de los medios virtuales

1. Haga clic en **Herramientas→ Iniciar Medios virtuales**.
2. Deseleccione la casilla que está junto a los medios que desea desconectar.

   Los medios se desconectan y se actualiza la ventana de **estado**.
3. Haga clic en **Salir** para terminar el asistente **Sesión de medios virtuales**.

NOTA: Siempre que se inicia una sesión de medios virtuales o se conecta una unidad vFlash, aparece una unidad adicional denominada "LCDRIVE" en el sistema operativo del host y en el BIOS. La unidad adicional desaparece cuando la unidad vFlash o la sesión de medios virtuales se desconectan.

Inicio desde los medios virtuales

El BIOS del sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disco virtuales. Durante la POST, 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 configuración del 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 <Intro>.

   En la ventana emergente, aparece una lista de las unidades ópticas virtuales y de discos virtuales con los dispositivos estándar de inicio.
4. Asegúrese de que la unidad virtual esté activada y que aparezca como el primer dispositivo con un medio de inicio. 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 de inicio con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio de inicio está presente, el sistema se inicia a partir del dispositivo virtual. De lo contrario, el sistema ignora el dispositivo; como ocurriría con un dispositivo físico que no tiene medios de inicio.

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 completarse. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de **medios virtuales** puede tardar menos de 15 minutos en completarse. Ver "Implementación del sistema operativo" en la página 265 para obtener más información.

1. Verifique lo siguiente:
   - El CD de instalación del 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" en la página 289 para asegurarse de que el BIOS esté configurado para iniciar desde la unidad de CD a partir de la que se realiza la instalación.
3. Siga las instrucciones que aparecen 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 no funcione, si inserta un nuevo CD/DVD en la unidad óptica remota sin realizar la reasignación.

Función Inicio único

La función Inicio único ayuda a cambiar el orden de 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.

Para usar la función Inicio único, haga lo siguiente:

1. Conéctese al iDRAC6 por medio de la interfaz web y haga clic en **Sistema→ Consola/Medios→ Configuración**.
2. Seleccione la opción **Activar el inicio una vez** en **Medios virtuales**.
3. Encienda el servidor e ingrese al administrador de inicio del BIOS.
4. Cambie la secuencia de inicio para iniciar desde el dispositivo de medios virtuales remoto.
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 se desconecta.

   NOTA: Los medios virtuales deben estar en estado **Conectado** para que las unidades virtuales aparezcan en la secuencia de inicio. Verifique que los medios de inicio estén presentes en la unidad virtualizada para activar la opción **Iniciar una vez**.

Uso de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En los sistemas Windows, las unidades de medios virtuales se montan automáticamente si están conectadas y configuradas con una letra de unidad.

El uso de las unidades virtuales desde Windows es similar al uso de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estar disponibles en el sistema haciendo clic en la unidad y examinando el contenido de la misma.

Sistemas basados en 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 14-3 contiene las preguntas y respuestas frecuentes.

Tabla 14-3. 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 se termina el tiempo de espera en 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 compatibles" en la página 28 para ver una lista de los sistemas operativos compatibles.
¿Qué exploradores web admiten el iDRAC6?	Consulte "Exploradores web admitidos" en la página 28 para ver una lista de los exploradores de web admitidos.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿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, el nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión si 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 se termina el tiempo de espera en 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 RACADM. Para restablecer la conexión con el disco virtual, use la función de **Medios virtuales**.
La instalación del sistema operativo Windows mediante los medios virtuales parece tardar demasiado. ¿Por qué?	Si instala el sistema operativo Windows por medio del DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) 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. Aunque la ventana de instalación no indique el progreso de la instalación, el procedimiento de instalación está teniendo lugar.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cómo configuro mi dispositivo virtual como dispositivo de inicio?	En el servidor administrado, acceda a la configuración del BIOS y haga clic en el menú de inicio. Localice el CD virtual, el disco virtual o la memoria vFlash y cambie el orden de los dispositivos de inicio según corresponda. Para configurar el dispositivo virtual como dispositivo de inicio, 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 ésta como la primera unidad en el orden de inicio.
¿Desde 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 disco flexible o disco flexible 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 de inicio?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para que la memoria USB de Dell funcione como dispositivo de inicio. 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 el símbolo del sistema de DOS, escriba el comando siguiente: `sys a: x: /s` donde *x*: es la memoria USB que desea hacer de inicio.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
No puedo encontrar mi dispositivo de disco flexible 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 disco flexible remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disco virtual y la unidad de CD virtual de manera similar. Para montar la unidad de disco flexible virtual, encuentre el nodo de dispositivo que Linux asigna a la unidad de disco flexible virtual. Realice los pasos siguientes para encontrar y montar correctamente la unidad de disco flexible virtual: **1** Abra un símbolo del sistema de Linux y ejecute el siguiente comando: `grep "Disco virtual" /var/log/messages` **2** Localice la última entrada de dicho mensaje y anote la hora. **3** En la línea de comandos 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 flexible virtual Dell. **5** Asegúrese de que está conectado a la unidad de disco flexible virtual. **6** En la línea de comandos de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: `/dev/sdx` es el nombre del dispositivo que se encontró en el paso 4 `/mnt/floppy` es el punto de montaje.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta

No puedo encontrar mi dispositivo de disco flexible 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 disco flexible 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 un 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 línea de comandos de Linux, ejecute el siguiente comando:
	`grep "hh:mm:ss" /var/log/messages`
	donde
	`hh:mm:ss` es la fecha y hora del mensaje devuelto por el comando `grep` en el paso 1.
	4 En el paso 3, lea el resultado del comando grep y localice el nombre del dispositivo que se asignó a *CD virtual de Dell*.
	5 Asegúrese de que está conectado a la unidad de CD virtual.
	6 En la línea de comandos de Linux, ejecute el siguiente comando:
	`mount /dev/sdx /mnt/CD`
	donde:
	`/dev/sdx` es el nombre del dispositivo que se encontró en el paso 4
	`/mnt/floppy` es el punto de montaje.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
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 de vFlash están conectados como un dispositivo USB compuesto al BUS USB del host y comparten un puerto USB común. Cuando un medio virtual o un dispositivo USB vFlash se conecta o se desconecta del BUS USB del host, todos los medios virtuales y los dispositivos vFlash 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 vFlash. Se recomienda conectar 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.

Tabla 14-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cómo puedo obtener el máximo rendimiento de los medios virtuales?	Para obtener el máximo rendimiento de los medios virtuales, inicie los medios virtuales con la consola virtual desactivada o realice alguna de las siguientes acciones: • Reduzca la resolución del vídeo y la intensidad del color de la pantalla de la consola virtual al mínimo posible. • Desactive el cifrado tanto para los medios virtuales como para la consola virtual. **NOTA:** En este caso, la transferencia de datos entre el servidor administrado y el iDRAC para los medios virtuales y la consola virtual estará asegurada. • Si está utilizando un sistema operativo de servidor Windows, detenga el servicio de Windows denominado Recopilador de sucesos de Windows. Para hacer esto, vaya a **Inicio > Herramientas administrativas > Servicios**. Haga clic con el botón derecho del mouse en **Recopilador de sucesos de Windows** y haga clic en **Detener**.

15

Configuración de la tarjeta vFlash SD y administración de las particiones vFlash

La tarjeta vFlash SD es una tarjeta digital segura (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 dispositivo USB flash común. Es el lugar de almacenamiento de las particiones definidas por el usuario que se pueden configurar para exponerlas al sistema como dispositivos USB y también usarlas para crear un dispositivo USB de inicio. Según el modo de emulación seleccionado, las particiones se presentarán al sistema como una unidad de disco flexible, un disco duro o una unidad CD/DVD. Cualquiera de éstos puede definirse como dispositivo de inicio.

Para obtener información sobre cómo instalar y desinstalar la tarjeta del sistema, consulte el *Manual del propietario de hardware* en **dell.com/support/manuals**.

Se admiten tarjetas vFlash SD y tarjetas SD estándar. Una *tarjeta vFlash SD* es una tarjeta que admite las nuevas funciones vFlash mejoradas. Una *tarjeta SD estándar* es una tarjeta SD normal genérica que sólo admite algunas funciones de vFlash.

Con una tarjeta vFlash SD se pueden crear hasta 16 particiones. Se puede asignar un nombre de etiqueta a la partición al crearla, y es posible realizar diversas operaciones para administrar y utilizar las particiones. Una tarjeta vFlash SD puede ser de cualquier tamaño hasta 8 GB. El tamaño de cada partición puede ser de hasta 4 GB.

Una tarjeta SD estándar puede ser de cualquier tamaño, pero sólo admite una partición. El tamaño de la partición está limitado a 256 MB. El nombre de la etiqueta de la partición es VFLASH de forma predeterminada.

NOTA: Asegúrese de insertar solamente una tarjeta vFlash SD o una tarjeta SD estándar en la ranura para tarjeta de iDRAC6 Enterprise. Si inserta una tarjeta de cualquier otro formato (por ejemplo, una tarjeta multimedia [MMC]), aparece el siguiente mensaje de error al inicializar la tarjeta: *Se ha producido un error al inicializar la tarjeta SD.*

Si es un administrador, puede realizar todas las operaciones en las particiones vFlash. Si no lo es, debe tener privilegios para acceder a los medios virtuales para poder crear, eliminar, formatear, conectar, desconectar o copiar el contenido de la partición.

Configuración de la tarjeta SD estándar o vFlash mediante la interfaz web del iDRAC6

Después de instalar la tarjeta SD estándar o vFlash, puede ver sus propiedades, activar o desactivar vFlash e inicializar la tarjeta. La funcionalidad vFlash debe estar activada para realizar la administración de particiones. Cuando la tarjeta está desactivada, sólo es posible ver sus propiedades. La operación de inicialización elimina las particiones existentes y restablece la tarjeta.

NOTA: Debe tener permiso para configurar el iDRAC para activar o desactivar vFlash, o para poder inicializar la tarjeta.

Si la tarjeta no está disponible en la ranura para tarjeta del iDRAC6 Enterprise del sistema, aparece el siguiente mensaje de error.

```
No se detectó la tarjeta SD. Inserte una tarjeta SD de
256 MB de tamaño o superior.
```

Para ver y configurar la tarjeta SD estándar o vFlash:

1. Abra un explorador web compatible e inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Sistema** en el árbol del sistema.
3. Haga clic en la ficha **vFlash**. Aparece la página **Propiedades de la tarjeta SD**.

En la Tabla 15-1 se enumeran las propiedades mostradas para la tarjeta SD.

Tabla 15-1. Propiedades de la tarjeta SD

Atributo	Descripción
Name (Nombre)	Muestra el nombre de la tarjeta insertada en la ranura para tarjeta del iDRAC6 Enterprise del servidor. Si la tarjeta admite las nuevas funciones mejoradas de vFlash, muestra *Tarjeta vFlash SD*. Si admite funciones limitadas de vFlash, muestra *Tarjeta SD*.
Tamaño	Muestra el tamaño de la tarjeta en gigabytes (GB).
Available Space	Muestra el espacio no utilizado en la tarjeta vFlash SD en MB. Este espacio está disponible para crear más particiones en la tarjeta vFlash SD. Si la tarjeta vFlash SD insertada no está inicializada, el espacio disponible muestra que la tarjeta está sin inicializar. Para la tarjeta SD estándar, el espacio disponible no se muestra.
Protegido contra escritura	Muestra si la tarjeta está protegida contra escritura o no.
Condición	Muestra la condición general de la tarjeta vFlash SD. Ésta puede ser: • En buen estado • Aviso • Critical (Crítico) Si es un aviso, reinicialice la tarjeta. Si es crítico, reinstale y reinicialice la tarjeta. Para la tarjeta SD estándar, la condición no se muestra.
vFlash activado	Seleccione la casilla de marcación para administrar la partición vFlash de la tarjeta. Quite la marca de la casilla de marcación para desactivar la administración de la partición vFlash.

4 Haga clic en **Aplicar** para activar o desactivar la administración de la partición vFlash en la tarjeta.

Si hay alguna partición vFlash conectada, no es posible desactivar vFlash y aparece un mensaje de error.

NOTA: Si vFlash está desactivado, sólo aparece la subficha **Propiedades de la tarjeta SD**.

5 Haga clic en **Inicializar**. Se eliminan todas las particiones existentes y la tarjeta se restablece. Aparece un mensaje de confirmación.

6 Haga clic en **OK** (Aceptar). Una vez que la operación de inicialización se completa, aparece un mensaje de inicialización satisfactoria.

NOTA: La inicialización se activa sólo si se selecciona la opción **vFlash activada**.

Si hay alguna partición vFlash conectada, la operación de inicialización falla y aparece un mensaje de error.

Si hace clic en cualquier opción de las páginas de vFlash mientras una aplicación como el proveedor de WSMAN, la utilidad de configuración del iDRAC6 o racadm está utilizando vFlash, o si se desplaza a alguna otra página en la interfaz gráfica de usuario, el iDRAC6 puede mostrar el siguiente mensaje:

`vFlash está siendo utilizado actualmente por otro proceso. Intente de nuevo más tarde.`

Configuración de una tarjeta SD estándar o vFlash utilizando racadm

Se puede ver y configurar la tarjeta SD estándar o vFlash utilizando comandos de racadm desde una consola local, remota o Telnet/SSH.

NOTA: Debe tener permiso para configurar el iDRAC para activar o desactivar vFlash, y para inicializar la tarjeta.

Cómo mostrar las propiedades de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando:

```
racadm getconfig -g cfgvFlashSD
```

Aparecen las siguientes propiedades de sólo lectura:

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`

- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

Activación o desactivación de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca los siguientes comandos:

- Para activar una tarjeta SD estándar o vFlash:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- Para desactivar una tarjeta SD estándar o vFlash:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
  ```

NOTA: El comando racadm sólo funciona si hay una tarjeta SD estándar o vFlash presente. Si no hay una tarjeta presente, aparece el siguiente mensaje: *ERROR: No hay tarjeta SD presente* .

Inicialización de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando para inicializar la tarjeta:

```
racadm  vflashsd  initialize
```

Se eliminan todas las particiones existentes y la tarjeta se restablece.

Obtención del último estado de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando para obtener el estado del último comando de inicialización enviado a la tarjeta SD estándar o vFlash:

```
racadm vFlashsd status
```

NOTA: Este comando sólo muestra el estado de los comandos enviados a la tarjeta SD. Para obtener el estado de los comandos enviados a las particiones individuales en la tarjeta SD, utilice el comando:

```
racadm vflashpartition status
```

Restablecimiento de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca:

```
racadm vflashsd initialize
```

Para obtener más información sobre `vflashsd`, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) en el sitio web del servicio de asistencia de Dell en **dell.com/support/manuals**.

NOTA: El comando `racadm vmkey reset` se ha descartado a partir de la versión 1.5. La funcionalidad de este comando está cubierta ahora por `vflashsd initialize`. Aunque la ejecución del comando `vmkey reset` será satisfactoria, se recomienda utilizar el comando `vflashsd initialize`. Para obtener más información, consulte "Inicialización de la tarjeta SD estándar o vFlash" en la página 303.

Administración de las particiones vFlash mediante la interfaz web del iDRAC6

Puede realizar las siguientes tareas:

- Crear una partición vacía
- Crear una partición utilizando un archivo de imagen
- Formatear una partición
- Ver las particiones disponibles
- Modificar una partición
- Adjuntar/separar una partición
- Eliminar las particiones existentes
- Descargar el contenido de una partición
- Iniciar una partición

Creación de una partición vacía

Una partición vacía es similar a una memoria USB vacía. Se pueden crear particiones vacías en una tarjeta SD estándar o vFlash. Se puede elegir crear una partición de tipo *disco flexible* o *disco duro*. No está admitido el tipo de partición CD en la creación de particiones vacías.

NOTA: Debe tener privilegios de acceso a los medios virtuales para crear particiones vacías.

Antes de crear una partición vacía, asegúrese de lo siguiente:

- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Para crear una partición vFlash vacía:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Crear partición vacía**. Aparece la página **Crear partición vacía**.
2. Introduzca la información que se indica en Tabla 15-2.
3. Haga clic en **Aplicar**. Se crea una nueva partición. Aparece una página que indica el progreso en porcentaje.

   Aparece un mensaje de error si:

   - La tarjeta está protegida contra escritura.
   - El nombre de la etiqueta coincide con la etiqueta de una partición existente.
   - Se introduce un valor no entero para el tamaño de la partición, el valor excede el espacio disponible en la tarjeta o el tamaño de la partición es mayor que 4 GB.
   - Ya se está realizando una operación de inicialización en la tarjeta.

   NOTA: La nueva partición no está formateada (RAW).

Tabla 15-2. Opciones de la página Creación de una partición vacía

Campo	Descripción
Índice	Seleccione un índice de partición. Sólo se muestran los índices no utilizados en la lista desplegable. En forma predeterminada, se selecciona el índice disponible más bajo. Puede cambiarlo a cualquier otro valor de índice de la lista desplegable. **NOTA:** Para la tarjeta SD estándar, sólo está disponible el índice 1.

Tabla 15-2. Opciones de la página Creación de una partición vacía *(continuación)*

Campo	Descripción
Etiqueta	Introduzca una etiqueta exclusiva para la nueva partición. El nombre de la etiqueta puede contener hasta seis caracteres alfanuméricos. No incluya ningún espacio en el nombre de la etiqueta. Los caracteres se muestran en mayúsculas. **NOTA:** Para la tarjeta SD estándar, el nombre de la etiqueta es VFLASH de manera predeterminada, y este nombre no se puede cambiar.
Tipo de emulación	Seleccione el tipo de emulación para la partición en la lista desplegable. Las opciones disponibles son **Disco flexible** y **Disco duro**.
Tamaño	Introduzca el tamaño de la partición en megabytes (MB). El tamaño máximo de la partición es de 4 GB, o menor o igual que el espacio disponible en la tarjeta vFlash SD. **NOTA:** Para la tarjeta SD estándar, el tamaño de la partición es de 256 MB, y no se puede cambiar.

Creación de una partición utilizando un archivo de imagen

Se puede crear una nueva partición en la tarjeta SD estándar o vFlash utilizando un archivo de imagen (disponible en formato **.img** o **.iso**). Se puede crear una partición de tipo disco flexible, disco duro o CD.

NOTA: Para crear particiones debe tener privilegios de acceso a medios virtuales.

Si se utiliza un archivo de imagen **.iso** (para CD), se crea una partición de sólo lectura. Si se utiliza un archivo de imagen **.img** (para disco flexible y disco duro), se crea una partición de lectura y escritura.

El tamaño de la partición recién creada es igual al tamaño del archivo de imagen. El tamaño del archivo de imagen debe ser:

- Menor o igual que el espacio disponible en la tarjeta.
- Menor o igual a 4 GB. El tamaño máximo de la partición es de 4 GB.

Utilizando la interfaz web, el tamaño de imagen que se puede cargar en la tarjeta vFlash SD está limitado a un máximo de 2 GB en exploradores de 32 bits y de 64 bits (Internet Explorer y FireFox).

Utilizando la interfaz de racadm y WSMAN, el tamaño de la imagen que se puede cargar en la tarjeta vFlash SD es de un máximo de 4 GB.

Para la tarjeta SD estándar, el tamaño de la imagen debe ser menor o igual a 256 MB.

Antes de crear una partición para un archivo de imagen, asegúrese de lo siguiente:

- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

NOTA: Al crear una partición desde un archivo de imagen, asegúrese de que el tipo de imagen y el tipo de emulación coincidan. iDRAC emula la imagen como el tipo de imagen especificado. Podría haber problemas cuando la imagen cargada y el tipo de emulación no coinciden. Por ejemplo, si la partición se crea utilizando una imagen ISO y el tipo de emulación se especifica como disco duro, entonces el BIOS no podrá iniciarse a partir de esta imagen.

Para crear una partición vFlash utilizando un archivo de imagen:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Crear desde imagen**. Aparece la página **Crear partición desde un archivo de imagen**.
2. Introduzca la información que se indica en Tabla 15-3.
3. Haga clic en **Aplicar**. Se crea una nueva partición.

   Aparece un mensaje de error si:

   - La tarjeta está protegida contra escritura.
   - El nombre de la etiqueta coincide con la etiqueta de una partición existente.
   - El tamaño de la imagen es mayor de 4 GB o excede el espacio disponible en la tarjeta.
   - El archivo de imagen no existe o la extensión del archivo de imagen no es **.img** ni **.iso**.
   - Ya se está realizando una operación de inicialización en la tarjeta.

Tabla 15-3. Opciones de la página Creación de una partición desde un archivo de imagen

Campo	Descripción
Índice	Seleccione un índice de partición. Sólo se muestran los índices no utilizados en la lista desplegable. En forma predeterminada, se selecciona el índice disponible más bajo. Puede cambiarlo a cualquier otro valor de índice de la lista desplegable. **NOTA:** Para la tarjeta SD estándar, sólo está disponible el índice 1.
Etiqueta	Introduzca una etiqueta exclusiva para la nueva partición. Ésta puede contener hasta seis caracteres alfanuméricos. No incluya espacios en el nombre de la etiqueta. Los caracteres se muestran en mayúsculas. **NOTA:** Para la tarjeta SD estándar, el nombre de la etiqueta es VFLASH y no se puede modificar.
Tipo de emulación	Seleccione el tipo de emulación para la partición en la lista desplegable. Las opciones disponibles son **Disco flexible**, **Disco duro** y **CD**.
Ubicación de la imagen	Haga clic en **Examinar** y especifique la ubicación del archivo de imagen. Sólo se admiten los tipos de archivo **.img** o **.iso**.

Formateo de una partición

Se puede formatear una partición existente en la tarjeta vFlash SD con base en el tipo de sistema de archivos. Los tipos de sistemas de archivos admitidos son EXT2, EXT3, FAT16 y FAT32. La tarjeta SD estándar con funciones de vFlash limitadas admite sólo el formato FAT32.

Sólo se pueden formatear particiones de tipo Disco duro o Disco flexible. El formateo de particiones de tipo CD no se admite. No se pueden formatear las particiones de sólo lectura.

NOTA: Debe tener privilegios de acceso a los medios virtuales para formatear particiones.

Antes de formatear la partición, asegúrese de lo siguiente:

- La tarjeta está activada.
- La partición no está conectada.

- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Para formatear la partición vFlash:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Formatear**. Aparece la página **Formatear partición**.
2. Introduzca la información que se indica en Tabla 15-4.
3. Haga clic en **Aplicar**. Aparece un mensaje de advertencia que indica que todos los datos de la partición se borrarán. Haga clic en **OK** (Aceptar). La partición seleccionada se formatea conforme al tipo de sistema de archivos especificado.

   Aparece un mensaje de error si:

   - La tarjeta está protegida contra escritura.
   - Ya se está realizando una operación de inicialización en la tarjeta.

Tabla 15-4. Opciones de la página Formatear partición

Campo	Descripción
Etiqueta	Seleccione la etiqueta de la partición que desea formatear. Se selecciona la primera partición disponible de manera predeterminada. Todas las particiones existentes de tipo disco flexible o disco duro están disponibles en la lista desplegable. Las particiones que no están conectadas o que son de sólo lectura no están disponibles en la lista desplegable.
Tipo de formato	Seleccione el tipo de sistema de archivos conforme al que desea formatear la partición. Las opciones disponibles son EXT2, EXT3, FAT16 y FAT32.

Visualización de las particiones disponibles

Compruebe que la tarjeta SD estándar o vFlash está activada para ver la lista de particiones disponibles.

Para ver las particiones disponibles en la tarjeta:

1. En la interfaz web del iDRAC6, seleccione **Sistema→ vFlash** subficha→ **Administrar**. En la página **Administrar particiones** se enumeran las particiones disponibles.

2 Para cada partición, se puede ver la información incluida en la Tabla 15-5.

Tabla 15-5. Visualización de las particiones disponibles

Campo	Descripción
Índice	Las particiones tienen un número de índice de 1 a 16. El índice de la partición es exclusivo para una partición específica. Se especifica cuando se crea una partición.
Etiqueta	Identifica la partición. Se especifica cuando se crea una partición.
Tamaño	Tamaño de la partición en megabytes (MB).
Sólo lectura	Estado del acceso de lectura y escritura de la partición. • Marcado = Partición de sólo lectura. • No marcado = Partición de lectura y escritura. **NOTA:** Para la tarjeta SD estándar, la partición es de lectura y escritura, y esta columna no aparece.
Conectado	Indica si la partición es visible para el sistema operativo como un dispositivo USB. Para conectar o desconectar las particiones, consulte la sección "Cómo conectar y desconectar una partición" en la página 311.
Escriba	Muestra si el tipo de la partición es disco flexible, disco duro o CD.
Estado	Estado de una operación en curso o de la última operación realizada en la partición con el porcentaje del progreso. Los valores del estado son: • Inactivo: no se está realizando ninguna operación. • Formateando: la partición se está formateando. • Creando: la partición se está creando.

Modificación de una partición

Asegúrese de que la tarjeta esté activada para modificar la partición.

Se puede cambiar una partición de sólo lectura a lectura y escritura, y viceversa. Para hacer esto:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Sólo lectura**, seleccione la casilla de marcación para las particiones que desea cambiar a sólo lectura o quite la marca de las casillas de marcación que desea cambiar a lectura y escritura.

   NOTA: Si la partición es de tipo CD, el estado es sólo lectura y la casilla de marcación está seleccionada de manera predeterminada. El estado no se puede cambiar a lectura y escritura.
   Si la partición está conectada, la casilla de marcación aparece en gris.
   Para la tarjeta SD estándar, la partición es de lectura y escritura, y la columna **Sólo lectura** no aparece.
3. Haga clic en **Aplicar**. Las particiones se cambian a sólo lectura o lectura y escritura con base en las selecciones.

Cómo conectar y desconectar una partición

Se pueden conectar una o más particiones como un dispositivo de almacenamiento masivo USB virtual, de forma que sean visibles para el sistema operativo y el BIOS como dispositivos de almacenamiento masivo. Cuando se conectan varias particiones simultáneamente, se presentan en orden ascendente al sistema operativo host según el índice. El sistema operativo controla la asignación de la letra de unidad correspondiente.

Si se desconecta una partición, ya no se ve como un dispositivo de almacenamiento masivo USB virtual en el sistema operativo host y se elimina del menú de orden de inicio del BIOS.

Si se está conectando o desconectando una partición, el bus USB del sistema se restablece. Esto puede afectar a las aplicaciones (como el sistema operativo) que estén utilizando vFlash, y se desconectan las sesiones de medios virtuales del iDRAC.

NOTA: Debe tener privilegios de acceso a los medios virtuales para conectar o desconectar una partición.

Antes de conectar o desconectar una partición, asegúrese de lo siguiente:

- La tarjeta está activada.
- No se está realizando una operación de inicialización en la tarjeta.

Para conectar o desconectar particiones:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Conectada**, seleccione la casilla de marcación para las particiones que desea conectar, o quite la marca de la casilla de marcación para las particiones que desea desconectar.

   NOTA: Las particiones desconectadas no aparecen en la secuencia de inicio.
3. Haga clic en **Aplicar**. Las particiones se conectan o desconectan conforme a las selecciones.

Comportamiento del sistema operativo para particiones conectadas

Cuando las particiones están conectadas y el sistema operativo host es Windows, el sistema operativo controla las letras de unidad que se asignan a las particiones conectadas.

Si una partición es de sólo lectura, sólo podrá leer como se ve en el sistema operativo host.

Si el sistema operativo host no admite el sistema de archivos de una partición conectada, no se puede leer ni modificar el contenido de la partición desde el sistema operativo host. Por ejemplo, una partición de tipo EXT2 no se puede leer desde el sistema operativo Windows.

Cuando se cambia el nombre de la etiqueta de una partición conectada desde el sistema operativo host, esto no afecta el nombre de la etiqueta almacenado en el iDRAC para esa partición.

Eliminación de las particiones existentes

NOTA: Las particiones existentes se pueden eliminar en la tarjeta SD estándar o vFlash.

Antes de eliminar las particiones existentes, compruebe lo siguiente:

- La tarjeta está activada.
- La tarjeta no está protegida contra escritura.

- La partición no está conectada.
- No se está realizando una operación de inicialización en la tarjeta.

Para eliminar las particiones existentes:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Eliminar**, haga clic en el icono Eliminar para las particiones que desee eliminar y luego haga clic en **Aplicar**. Las particiones se eliminan.

Descarga del contenido de una partición

El contenido de una partición vFlash se puede descargar en una ubicación local o remota como un archivo de imagen en formato **.img** o **.iso**. Una ubicación local es en el sistema de administración desde el que se opera la interfaz web del iDRAC6. Una ubicación remota es una ubicación de red asignada a la estación de administración.

NOTA: Debe tener privilegios de acceso a los medios virtuales para descargar particiones.

Antes de descargar el contenido a una ubicación local o remota, asegúrese de lo siguiente:

- La tarjeta está activada.
- No se está realizando una operación de inicialización en la tarjeta.
- En el caso de una partición de lectura y escritura, no debe estar conectada.

Para descargar el contenido de la partición vFlash a una ubicación en su sistema:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Descargar**. Aparece la página **Descargar partición**.
2. Desde el menú desplegable **Etiqueta**, seleccione una partición que desee descargar. Todas las particiones existentes se muestran en la lista, excepto las particiones que están conectadas. Se selecciona la primera partición de manera predeterminada.
3. Haga clic en **Descargar**.
4. Especifique la ubicación donde desea guardar el archivo.

Si sólo se especifica la ubicación de la carpeta, la etiqueta de la partición se usa como nombre del archivo, junto con la extensión **.iso** para las particiones de tipo CD y la extensión **.img** para las particiones de tipo disco flexible o disco duro.

5 Haga clic en **Save** (Guardar). El contenido de la partición seleccionada se descarga en la ubicación especificada.

Inicio de una partición

Se puede establecer una partición vFlash conectada como el dispositivo de inicio para la siguiente operación de inicio. La partición vFlash debe contener una imagen de inicio (en formato **.img** o **.iso**) para establecerla como dispositivo de inicio. Asegúrese de que la tarjeta esté activada para establecer una partición como dispositivo de inicio y realizar la operación de inicio.

NOTA: Debe tener privilegios de acceso a los medios virtuales para establecer una partición como el dispositivo de inicio.

Puede realizar la operación de inicio para la tarjeta SD estándar o vFlash. Para ver los pasos, consulte la sección "Primer dispositivo de inicio" en la página 86.

NOTA: Si el BIOS del sistema no admite vFlash como el primer dispositivo de inicio, es posible que las particiones vFlash conectadas no se encuentren en el menú desplegable **Primer dispositivo de inicio**. Por lo tanto, asegúrese de actualizar el BIOS con la versión más reciente que admita el establecimiento de la partición vFlash como el primer dispositivo de inicio. Si el BIOS es de la versión más reciente, al reiniciar el servidor el BIOS informa al iDRAC que admite vFlash como primer dispositivo de inicio y el iDRAC presenta la partición vFlash en el menú desplegable **Primer dispositivo de inicio**.

Administración de particiones vFlash mediante racadm

Se puede utilizar el subcomando `vFlashPartition` para crear, eliminar, enumerar o ver el estado de las particiones en una tarjeta SD estándar o vFlash ya inicializada. El formato es:

```
racadm vflashpartition <create | delete | status |
list> <options>
```

NOTA: Debe tener privilegios de acceso a los medios virtuales para llevar a cabo la administración de las particiones vFlash.

Opciones válidas:

-i <index>	Índice de la partición para la que se aplica este comando. <index> debe ser un número entero entre 1 y 16. **NOTA:** Para la tarjeta SD estándar, el valor del índice se limita a 1 porque sólo se admite una partición de 256 MB.

Opciones que sólo son válidas con la acción "crear":

-o <label>	La etiqueta que se muestra cuando la partición se monta en un sistema operativo. <label> debe ser una cadena de hasta seis caracteres alfanuméricos y no debe contener espacios.
-e <type>	Tipo de emulación para la partición. <type> debe ser disco flexible, cddvd o HDD.

-t <type>	Creación de un participación de tipo <tipo>. <type> debe ser:
	• Vacío: crear una partición vacía.
	  • -s <size>: tamaño de la partición en MB.
	  • -f <type>: tipo de formato para la partición con base en el tipo de sistema de archivos. Las opciones válidas son RAW, FAT16, FAT32, EXT2 ó EXT3.
	• Imagen: crear una partición utilizando una imagen relativa al iDRAC. Las siguientes opciones son válidas con el tipo de imagen:
	  • -l <path>: especifica la ruta de acceso remota relativa al iDRAC. La ruta de acceso puede estar en una unidad montada:
	  Ruta de acceso de SMB: //<ip or domain>/<share_name> /<path_to_image>
	  Ruta de acceso de NFS: <ipaddress>:/<path_to_image>
	  • -u <user>: nombre de usuario para acceder a la imagen remota.
	  • -p <password>: contraseña para acceder a la imagen remota.

Opciones que sólo son válidas con la acción "estado":

-a	Muestra el estado de las operaciones en todas las particiones existentes.

Creación de una partición

- Para crear una partición vacía de 20 MB:

  ```
  racadm vflashpartition create -i 1 -o drive1 -t
  empty -e HDD -f fat16 -s 20
  ```

- Para crear una partición utilizando un archivo de imagen de un sistema remoto:

  ```
  racadm vflashpartition create –i 1 –o drive1 –e
  HDD –t image –l //mi_servidor/sharedfolder/foo.iso
  –u root –p mi_contraseña
  ```

  NOTA: Este comando distingue entre mayúsculas y minúsculas en la extensión de nombre de archivo de la imagen. Si la extensión de nombre de archivo está en mayúsculas, por ejemplo FOO.ISO en vez de FOO.iso, el comando devuelve un error de sintaxis.

NOTA: La creación de una partición utilizando un archivo de imagen no se admite en racadm local.

Eliminación de una partición

- Para eliminar una partición:

  ```
  racadm vflashpartition delete -i 1
  ```

- Para eliminar todas las particiones, reinicialice la tarjeta vFlash SD. Para obtener más información, ver "Inicialización de la tarjeta SD estándar o vFlash" en la página 303.

Cómo obtener el estado de una partición

- Para obtener el estado operativo en la partición 1:

  ```
  racadm vflashpartition status -i 1
  ```

- Para obtener el estado de todas las particiones existentes:

  ```
  racadm vflashpartition status -a
  ```

Visualización de la información de las particiones

Para enumerar todas las particiones existentes y sus propiedades:

```
racadm vflashpartition list
```

Inicio de una partición

- Para enumerar los dispositivos disponibles en la lista de inicio:

  ```
  racadm  getconfig -g cfgServerInfo -o
  cfgServerFirstBootDevice
  ```

  Si se trata de una tarjeta vFlash SD, los nombres de las etiquetas de las particiones conectadas aparecen en la lista de inicio. Si es una tarjeta SD estándar y la partición está conectada, aparece VFLASH en la lista de inicio.

- Para establecer una partición vFlash como dispositivo de inicio:

  ```
  racadm  config -g cfgServerInfo -o
  cfgServerFirstBootDevice "<vFlash partition name>"
  ```

  donde <vFlash partition name> es el nombre de la etiqueta para la tarjeta vFlash SD y VFLASH para la tarjeta SD estándar.

  NOTA: Cuando se ejecuta este comando, la etiqueta de la partición vFlash se establece automáticamente como inicio único, es decir, **cfgserverBootOnce** se establece como 1. Iniciar una vez inicia el dispositivo desde la partición sólo una vez y no persiste en mantenerlo primero en el orden de inicio.

Conexión o desconexión de una partición

- Para conectar una partición:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 1
  ```

- Para desconectar una partición:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 0
  ```

Modificación de una partición

- Para cambiar una partición de sólo lectura a lectura y escritura:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 1
  ```

- Para cambiar una partición de lectura y escritura a sólo lectura:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 0
  ```

Para obtener más información acerca de los subcomandos de racadm y las definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Preguntas frecuentes

¿Cuándo se bloquea la tarjeta SD estándar o vFlash?

El iDRAC bloquea los medios flash virtuales cuando la operación que está realizando requiere de acceso exclusivo a los medios. Por ejemplo, durante una operación de inicialización.

16

Supervisión y administración de la alimentación

Los sistemas Dell PowerEdge incorporan muchas características nuevas y mejoradas para la administración de la alimentación. El diseño de toda la plataforma, desde el hardware al firmware, pasando por 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:

- Suministros de energía y reguladores de voltaje de alta eficiencia 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 proporcionan muchas características para controlar y administrar la alimentación:

- **Presupuesto e inventario de alimentación:** durante el inicio, un inventario del sistema permite calcular el presupuesto de alimentación del sistema para 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 energía para reunir las mediciones 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 la perspectiva de utilización, podría tener una cantidad limitada de enfriamiento en el nivel de bastidor. Con un límite de alimentación definido por el usuario, se puede asignar la alimentación donde sea necesaria para cumplir con los requisitos de rendimiento.

El iDRAC6 supervisa el consumo de energía y dinámicamente regula los procesadores para que cumplan con su nivel límite definido, que maximiza el rendimiento y a su vez cumple con los requisitos de alimentación.

Supervisión de alimentación

El iDRAC6 supervisa el consumo de alimentación 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 alimentación
- Alimentación promedio, mínima y máxima
- Valores de capacidad adicional de alimentación
- Consumo de alimentación (también puede verse en gráficas en la interfaz web)

Configuración y administración de la alimentación

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. Específicamente, 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 encendido).
- Ver la información del presupuesto de alimentación para el servidor y las unidades de suministro de energía instaladas, como consumo de alimentación 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 **Suministros de energía** muestra el estado y la clasificación de las unidades de 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:
   - **Total**: los suministros de energía instalados en el sistema son del mismo tipo y están funcionando correctamente.
   - **Pérdida**: en sistemas con dos unidades de suministro de energía, si los suministros de energía instalados en el sistema son de tipos diferentes o si uno de ellos está fallando o se ha desconectado. En sistemas con cuatro unidades de suministro de energía, si los suministros de energía instalados en el sistema son de dos tipos diferentes o si dos o tres unidades están fallando o se han desconectado.
   - **Desactivada**: sólo uno de los suministros de energía está disponible. No existe redundancia.
   - **Degradada** (sólo en sistemas con cuatro unidades de suministro de energía): Hay cuatro unidades de suministro de energía instaladas en el sistema, pero una de ellas está fallando o se ha desconectado.
   - **Elementos de suministro de energía individuales:** los posibles valores son:
   - **Estado** muestra lo siguiente:
     - **En buen estado** indica que la unidad de suministro de energía está presente y 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 del 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 del suministro de energía, que es la carga máxima de corriente alterna que el sistema podría colocar en el centro de datos.

– **Potencia máxima** muestra la potencia máxima del 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 en buen estado pérdida de potencia, 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.

Cómo utilizar de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

Cómo ver el presupuesto de alimentación

El servidor proporciona descripciones generales del estado de presupuesto de alimentación del subsistema de energía en la página **Información del presupuesto de alimentación**.

Cómo utilizar 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 ficha **Alimentación**.
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 consumo de corriente alterna que se podría configurar como límite del sistema. Una vez seleccionado, este límite sería la carga de corriente alterna máxima que el sistema podría colocar en el centro de datos.

Consumo de alimentación mínima del sistema muestra el valor del límite inferior predeterminado de la alimentación.

Consumo de alimentación máxima del sistema muestra el valor del límite superior predeterminado de la alimentación. Este valor es también el consumo de alimentación máximo absoluto de la configuración actual del sistema.

Cómo utilizar 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 sobre cfgServerPower, incluidos los detalles de salida, consulte cfgServerPower en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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 alimentación cerca del umbral determinado. El consumo de alimentación 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 alimentación potencial máximo es 700 W y el consumo de alimentación 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 alimentación 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 ficha **Alimentación**.
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 **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 porcentual, será un porcentaje de intervalo de consumo de alimentación potencial máximo a mínimo. Por ejemplo, un umbral de 100% significa un consumo de alimentación potencial máximo, mientras que 0% significa un consumo de alimentación potencial mínimo.

   NOTA: El umbral de presupuesto de alimentación no puede ser mayor al consumo de alimentación potencial máximo ni menor al consumo de alimentación potencial mínimo.
5. Seleccione **Activar** para activar el umbral. El sistema implementará el umbral especificado por el usuario. Si borra la marca de la casilla, el sistema no tendrá un límite de alimentación.
6. Haga clic en **Aplicar cambios**.

Cómo utilizar de RACADM

```
racadm config -g cfgServerPower -o
cfgServerPowerCapWatts <power cap value in Watts>

racadm config -g cfgServerPower -o
cfgServerPowerCapBTUhr <power cap value in BTU/hr>

racadm config -g cfgServerPower -o
cfgServerPowerCapPercent <power cap value in %>

racadm config -g cfgServerPower -o
cfgServerPowerCapEnable <1 to enable, 0 to disable>
```

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.

Visualización de la supervisión de alimentación

Cómo utilizar 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. Aparece la página **Supervisión de alimentación**.

En la sección siguiente se describe la información proporcionada en la página **Supervisión de alimentación**:

Supervisión de alimentación

- **Estado**: **En buen estado** indica que las unidades 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 alimentación actual en vatios o BTU/h.

- **Umbral de advertencia**: muestra el consumo de energía aceptable (en vatios y BTU/h) recomendados para el funcionamiento del sistema. El consumo de energía que exceda este valor produce sucesos de advertencia.
- **Umbral de falla**: muestra el consumo de energía aceptable más alto (en vatios y BTU/h) requerido para el funcionamiento del sistema. El consumo de energía que exceda este valor produce sucesos de falla/críticos.

Amperaje

- **Ubicación**: muestra el nombre de la unidad de suministro de energía: PS-n donde n es el número del suministro de energía.
- **Lectura**: el consumo de alimentación actual en amperios.

Estadísticas de seguimiento de alimentación

- **Consumo de energía** indica el consumo acumulado actual de energía del servidor, medido en la entrada de los suministros de energía. El valor se expresa en KWh y es un valor acumulado que es el total de energía utilizada por el sistema. Se puede restablecer el valor con el botón **Restablecer**.
- **Alimentación pico del sistema** especifica el promedio máximo de 1 minuto de alimentación para el sistema desde la última hora inicial de medición. Se puede restablecer el valor con el botón **Restablecer**.
- **Amperaje pico del sistema** especifica el valor de corriente pico dentro del intervalo especificado por la hora de inicio y la hora pico. Se puede restablecer el valor con el botón **Restablecer**.
- La **Hora inicial de medición** muestra la fecha y la hora registradas cuando se borró por última vez el valor y comenzó el nuevo ciclo de mediciones. Para **Consumo de energía**, se puede restablecer este valor con el botón **Restablecer**, pero persistirá luego de un restablecimiento del sistema o de una operación de recuperación ante fallas. Para **Alimentación pico del sistema** y **Amperaje pico del sistema**, se puede restablecer este valor con el botón **Restablecer**, pero también persistirá luego de un restablecimiento o de una operación de recuperación ante fallas.

- La **Hora final de medición** muestra la fecha y hora actuales en las que se calculó el consumo de energía del sistema para mostrarlo. La **Hora pico** muestra la hora en la que se presentó la medición pico.

NOTA: Se mantienen estadísticas de seguimiento de alimentación luego de todos los restablecimientos del sistema para reflejar toda la actividad durante el intervalo entre la hora de inicio y de fin. El botón **Restablecer** restablecerá el campo respectivo y le asignará el valor cero. En la tabla siguiente, la información del consumo de alimentación no se mantiene a lo largo de los restablecimientos del sistema, por lo que se restablecerá a cero en dichas ocasiones. Los valores de alimentación que se muestran son promedios acumulados durante el intervalo de tiempo respectivo (minuto, hora, día y semana previos). Debido a que los intervalos de tiempo de inicio a 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.

Power Consumption

- Muestra el consumo de alimentación promedio, máximo y mínimo en el sistema para el último minuto, hora, día y semana.
- Consumo de alimentación promedio: promedio durante el minuto, la hora, el día y el mes anterior.
- Consumo de alimentación máximo y mínimo: los consumos de alimentación máximo y mínimo observados durante un intervalo de tiempo determinado.
- Hora de potencia máxima y mínima: la hora en la que se produjeron los consumos de alimentación máximo y mínimo.

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 alimentación 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 alimentación pico del sistema.

Mostrar gráfica

Haga clic en **Mostrar gráfica** para mostrar las gráficas que indican la potencia y el consumo de alimentación del iDRAC6 en vatios y en amperios, respectivamente, durante la última hora. El usuario tiene la opción de ver estas estadísticas hasta una semana antes, con el menú desplegable provisto sobre 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 potencia ni de consumo.

Cómo utilizar de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

Para obtener más información sobre **cfgServerPower**, incluidos los detalles de salida, consulte **cfgServerPower** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Ejecución de operaciones de control de alimentación en el servidor

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

El iDRAC6 le permite efectuar en forma remota varias acciones de administración de la alimentación, como un apagado ordenado.

Cómo utilizar la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en la ficha **Alimentación**. Aparecerá la página **Control de alimentación**.
3. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en el botón de radio:
   - **Encender el sistema** enciende el sistema (equivalente a pulsar el botón de encendido cuando el servidor está apagado). Esta opción está desactivada si el servidor ya está encendido.

- **Apagar el sistema** apaga la alimentación del servidor. Esta opción está desactivada si el sistema ya está apagado.
- **NMI (interrupción no enmascarable)** genera una NMI para interrumpir la operación del sistema.
- **Apagado ordenado** apaga el sistema.

  NOTA: Compruebe que la opción de apagado está configurada para el sistema operativo antes de realizar un apagado ordenado utilizando esta opción. Si utiliza esta opción sin configurarla en el sistema operativo, se reinicia el sistema administrado en lugar de realizar una operación de apagado.
- **Restablecer el sistema (reinicio mediante sistema operativo)** reinicia el sistema sin apagarlo. Esta acción está desactivada si el sistema ya está apagado.
- **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)** apaga el sistema y luego lo reinicia. Esta opción está desactivada si el sistema ya está apagado.

4 Haga clic en **Aplicar**. Aparece un cuadro de diálogo solicitando confirmación.

5 Haga clic en **Aceptar** para realizar la acción de administración de la alimentación (por ejemplo, hacer que se restablezca el sistema).

Cómo utilizar de RACADM

Abra una consola de texto de Telnet/SSH en el servidor, inicie sesión y escriba:

```
racadm serveraction <action>
```

donde `<action>` es powerup, powerdown, powercycle, hardreset o powerstatus.

17

Uso de la utilidad de configuración del iDRAC6

Descripción general

La utilidad de configuración del iDRAC6 es un entorno de configuración de preinicio que permite visualizar y establecer parámetros para iDRAC6 y para el servidor administrado. Específicamente, puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware del plano posterior primario
- Activar o desactivar la red de área local del iDRAC6
- Activar o desactivar la IPMI sobre LAN
- Configurar los parámetros de LAN
- Activar o desactivar el descubrimiento automático y configurar el servidor de aprovisionamiento
- Configurar los medios virtuales
- Configurar la tarjeta inteligente
- Cambiar el nombre de usuario y la contraseña del administrador
- Restablecer la configuración predeterminada de fábrica del iDRAC6
- Ver o borrar los mensajes del registro de eventos del sistema (SEL)
- Configurar LCD
- Configurar servicios del sistema

Las tareas que puede realizar con la utilidad de configuración del iDRAC6 también se pueden realizar mediante otras utilidades proporcionadas por el iDRAC6 o el software Dell OpenManage, incluyendo la interfaz basada en web, la interfaz de línea de comandos SM-CLP y la interfaz de línea de comandos de racadm local y remota.

Inicio de la utilidad de configuración del iDRAC6

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 presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el servidor e inténtelo otra vez.

Aparece la ventana de **Utilidad de configuración del iDRAC6**. Las dos primeras líneas ofrecen información sobre el firmware del iDRAC6 y las revisiones del firmware del plano posterior primario. Los niveles de revisión pueden ser útiles para determinar si necesita actualizar el firmware.

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 iDRAC6

Bajo los mensajes de revisión del firmware, el resto de la utilidad de configuración del iDRAC6 es un menú de opciones a las que puede tener acceso por medio de las teclas <Flecha hacia arriba> y <Flecha hacia abajo>.

- Si un elemento del menú conduce a un submenú o a un campo de texto editable, presione <Intro> para acceder al elemento y <Esc> para salir de él después de terminar de configurarlo.
- 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, aparece en azul. Algunos elementos se pueden editar en función de otras selecciones que se hagan.
- 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 iDRAC6, presione <Esc> para consultar 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 iDRAC6.

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, como por ejemplo, la interfaz basada en web, Telnet/SSH, la consola virtual y los medios virtuales.

Si elige desactivar la LAN, aparece la siguiente advertencia:

```
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 de los puertos HTTP, HTTPS, Telnet o SSH de iDRAC6, el tráfico de red de administración fuera de banda, como por ejemplo los mensajes de IPMI que se envían al iDRAC6 desde una estación de administración, no se reciben 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 acepta mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivada**, aparece la siguiente advertencia:

```
La interfaz del iDRAC6 fuera de banda se desactivará
si IPMI en la LAN está desactivada.
```

Presione cualquier tecla para quitar el mensaje y continuar. Ver “LAN del iDRAC6” en la página 333 para ver una explicación del mensaje.

Parámetros de la LAN

Presione <Intro> 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 17-1. Parámetros de la 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.
Prioridad de 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 <Intro> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Presione <Intro> 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.

Tabla 17-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
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** está **Desactivado**, presione <Intro> para modificar el campo de texto **Nombre de dominio actual**. Presione <Intro> cuando haya terminado de modificarlo. Presione <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.
Cadena del nombre del host	Presione <Intro> para editarla. Introduzca el nombre del host para alertas de captura de sucesos 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 IP donde se enviarán las alertas de PET de LAN.
Configuración de IPv4	Active o desactive la compatibilidad para conexión IPv4.
IPv4	Seleccione **Activado** o **Desactivado** para la compatibilidad con el protocolo IPv4.
Clave de cifrado RMCP+	Presione <Intro> 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 autentificación 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 toman el valor cero. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar.

Tabla 17-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
Dirección IP de Ethernet	Si la opción **Fuente de dirección IP** se establece como **DHCP**, este campo muestra la dirección IP que se obtuvo de DHCP. Si **Fuente 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 la opción **Fuente de dirección IP** se establece como **DHCP**, este campo muestra la dirección de máscara de subred que se obtuvo de DHCP. Si **Fuente 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 **Fuente 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 **Fuente 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.

Tabla 17-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
Dirección IPv6 1	Si **Fuente de dirección IP** se establece como **AutoConfig**, este campo muestra la dirección IP que se obtuvo de DHCP. Si **Fuente 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. Puede ser un valor entre 1 y 128, inclusive.
Puerta de enlace predeterminada	Si **Fuente 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 **Fuente de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada.
Dirección IPv6 de vínculo local	Ésta es la **dirección local de vínculo IPv6** no editable de la interfaz de red del iDRAC6.
Dirección IPv6 2	Esta es la **dirección IPv6 2** no editable de la interfaz de red del iDRAC6.
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 **Negociar automáticamente** se establece en **Desactivado**, seleccione entre 10 Mbps y 100 Mbps.
Configuración dúplex de LAN	Si **Negociar automáticamente** se establece en **Desactivado**, seleccione entre **Semidúplex** y **Dúplex completo**.

Configuración de soportes virtuales

Medios virtuales

Presione <Intro> y seleccione **Desconectado, Conectado** o **Autoconectado**. Cuando se selecciona **Conectado**, los dispositivos de medios virtuales se conectan al bus USB, haciéndolos disponibles para utilizarlos durante las sesiones de **Consola virtual**.

Si selecciona **Desconectado**, los usuarios no podrán acceder a los dispositivos de medios virtuales durante las sesiones de **Consola virtual**.

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 aparece como unidad de disco flexible en el sistema.

vFlash

Presione <Intro> para seleccionar **Activado** o **Desactivado**.

- **Activado**: vFlash está disponible para la administración de particiones.
- **Desactivado**: vFlash no está disponible para la administración de particiones.

PRECAUCIÓN: vFlash no se puede desactivar si una o más particiones están en uso o están conectadas.

Initialize vFlash

Elija esta opción para inicializar la tarjeta vFlash. La operación de inicialización borra los datos existentes en la tarjeta SD y todas las particiones existentes se eliminan. No puede realizar una operación de inicialización si una o más particiones están en uso o conectadas. Esta opción es accesible sólo si una tarjeta de un tamaño mayor que 256 MB está en la ranura para tarjetas de iDRAC Enterprise y si vFlash está activado.

Presione <Intro> para inicializar la tarjeta vFlash SD.

La operación de inicialización puede fallar debido a los siguientes motivos:

- La tarjeta SD no está presente actualmente.
- vFlash está siendo utilizado actualmente por otro proceso.

- vFlash no está activado.
- La tarjeta SD está protegida contra escritura.
- Una o más particiones están en uso actualmente.
- Una o más particiones están conectadas actualmente.

Propiedades de vFlash

Presione <Intro> para ver las siguientes propiedades de la tarjeta vFlash SD:

- **Nombre**: muestra el nombre de la tarjetavFlash SD insertada en la ranura para tarjeta vFlash SD del servidor. Si es una tarjeta SD Dell, dirá "vFlash SD Card". Si es una tarjeta SD que no es de Dell, dirá "SD Card".
- **Tamaño**: muestra el tamaño de la tarjeta vFlash SD en gigabytes (GB).
- **Espacio disponible**: muestra el espacio no utilizado en la tarjeta vFlash SD en megabytes (MB). Este espacio está disponible para crear más particiones en la tarjeta vFlash SD. Para las tarjetas SD, el espacio disponible aparece como 256 MB.
- **Protegido contra escritura**: muestra si la tarjeta vFlash SD está protegida contra escritura o no.
- **Condición**: muestra la condición general de la tarjeta vFlash SD. Ésta puede ser:
  - En buen estado
  - Aviso
  - Critical (Crítico)

Presione <Esc> para salir.

Inicio de sesión mediante tarjeta inteligente

Presione <Intro> para seleccionar **Activado** o **Desactivado**. Esta opción configura la característica de inicio de sesión mediante tarjeta inteligente. Las opciones disponibles son **Activado**, **Desactivado** y **Activado con RACADM**.

NOTA: Cuando seleccione **Activado** o **Activado con RACADM**, **IPMI en la LAN** se desactivará y bloqueará para edición.

Configuración de servicios del sistema

Servicios del sistema

Presione <Intro> para seleccionar **Activado** o **Desactivado**. Para obtener más información, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: Si modifica esta opción, el servidor se reinicia al seleccionar **Guardar** y **Salir** para aplicar la nueva configuración.

NOTA: Si elige restablecer los valores predeterminados de fábrica, la configuración para "Servicios del sistema" no cambia.

Cancelación de servicios del sistema

Presione <Intro> 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.

Recopilar el inventario del sistema en el reinicio

Seleccione la opción **Activado** para permitir la recopilación del inventario durante el reinicio. Para obtener más información, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: Si modifica esta opción, hará que el servidor se reinicie después de haber guardado la configuración y de haber salido de la utilidad de configuración de iDRAC6.

NOTA: Si elige restablecer los valores predeterminados de fábrica, la configuración de "Recopilar el inventario del sistema durante el reinicio" no cambia.

Configuración de LCD

Presione <Intro> para mostrar el submenú **Configuración de LCD**. Cuando haya terminado de configurar los parámetros de LCD, presione <Esc> para volver al menú anterior.

Tabla 17-2. Configuración de usuario de LCD

Línea 1 de LCD	Presione la <Flecha derecha>, <Flecha izquierda> y la barra espaciadora para cambiar entre las opciones. Esta función configura la pantalla **Inicio** en el LCD para una de las siguientes opciones: **Temp. ambiente, Etiqueta de propiedad, Nombre del 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	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	Seleccione **Vatio** o **BTU/h** para especificar la unidad que se mostrará en la pantalla LCD.
Unidades de temperatura ambiente para LCD	Seleccione **Celsius** o **Fahrenheit** para especificar la unidad que se mostrará en la pantalla LCD.
Pantalla de error de LCD	Seleccione **Simple** o **SEL** (registro de sucesos 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 suceso en idioma inglés. El formato SEL muestra una cadena de texto del registro de sucesos del sistema.
Indicación de la consola virtual remota en LCD	Seleccione **Activada** para mostrar el texto *Consola virtual* siempre que una consola virtual esté activa en la unidad.
Acceso al panel anterior de LCD	Presione <Flecha derecha>, <Flecha izquierda> y la barra espaciadora para cambiar entre las opciones: **Desactivado**, **Ver y modificar** y **Ver solamente**. Esta configuración define el nivel de acceso del usuario para la pantalla LCD.

Configuración de usuario de LAN

El usuario de la LAN es la cuenta de administrador del iDRAC6, que tiene el nombre predeterminado **root**. Presione <Intro> 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.

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, si se ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC6 a partir de la configuración predeterminada.

Presione <Intro> para seleccionar el elemento. Aparece el mensaje de advertencia siguiente:

```
Si restablece los valores predeterminados de fábrica
restaura la configuración no volátil de usuario
remoto. ¿Continuar?

< NO (Cancelar) >

< SÍ (Continuar) >
```

Seleccione **SÍ** y presione <Intro> para restablecer los valores predeterminados del iDRAC6.

Cualquiera de los mensajes de error siguientes aparece si esta operación falla:

- El comando de restablecimiento no fue satisfactorio. Por favor intente más tarde, el iDRAC está ocupado.
- No fue posible restablecer la configuración a los valores predeterminados; fin del tiempo de espera.
- No es posible enviar el comando Restablecer. Por favor intente más tarde, el iDRAC está ocupado.

Tabla 17-3. Configuración de usuario de LAN

Elemento	Descripción
Descubrimiento automático	El descubrimiento automático permite descubrir automáticamente sistemas no aprovisionados en la red y establece *de manera segura* las credenciales iniciales para administrar estos sistemas. Esta función permite al iDRAC6 localizar el servidor de aprovisionamiento. El iDRAC6 y el servidor de servicio de aprovisionamiento se autentifican el uno al otro. El servidor de aprovisionamiento remoto envía las credenciales del usuario para que el iDRAC6 genere una cuenta de usuario con esas credenciales. Una vez creada la cuenta de usuario, una consola remota puede establecer una comunicación WS-MAN con iDRAC6 utilizando las credenciales detalladas en el proceso de descubrimiento y luego enviar instrucciones seguras al iDRAC6 para instalar un sistema operativo de manera remota. Para obtener información sobre la implementación remota del sistema operativo, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**. Lleve a cabo los siguientes pasos previos en una sesión *independiente* de la **utilidad de configuración del iDRAC6** *antes de activar manualmente el descubrimiento automático*: • Activar la NIC • Activar IPv4 • Activar DHCP • Obtener el nombre de dominio de DHCP • Desactivar la cuenta de administrador (cuenta n.º 2) • Obtener la dirección de servidor DNS desde DHCP • Obtener el nombre de dominio DNS de DHCP Seleccionar **Activado** para activar la función de descubrimiento automático. De manera predeterminada, la opción aparece como **desactivado**. Si solicitó un sistema Dell con la función del descubrimiento automático **Activado**, el iDRAC6 del sistema Dell se suministrará con DHCP activado sin credenciales predeterminadas para un inicio de sesión remoto.

Tabla 17-3. Configuración de usuario de LAN *(continuación)*

Elemento	Descripción
Descubrimiento automático *(continuación)*	Antes de agregar el sistema Dell a la red y utilizar la función de descubrimiento automático, verifique los siguientes datos: • El servidor del protocolo de configuración dinámica de host (DHCP) y el sistema de nombres de dominio (DNS) están configurados. • Los servicios web de aprovisionamiento están instalados, configurados y registrados.
Servidor de aprovisionamiento	Este campo se utiliza para configurar el servidor de aprovisionamiento. La dirección del servidor de aprovisionamiento puede ser una combinación de direcciones IPv4 o nombre de host y no debe superar los 255 caracteres. Cada dirección debe estar separada por una coma. Si la función de descubrimiento automático está activada, y después de llevar a cabo el proceso de descubrimiento correctamente, las credenciales de usuario se obtienen del servidor de aprovisionamiento configurado para activar el aprovisionamiento remoto futuro. Para obtener más información, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.
Acceso a la cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione **Desactivado** para desactivar la cuenta de administrador o cuando el descubrimiento automático esté activado.
Privilegio de la cuenta	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Intro> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Escriba la contraseña nueva para la cuenta de administrador. Los caracteres no aparecen en la pantalla cuando los escribe.
Confirm Password (Confirmar la contraseña)	Escriba otra vez la contraseña nueva para la cuenta de administrador. Si los caracteres que introduce no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparece un mensaje y deberá introducir nuevamente la contraseña.

Menú del registro de sucesos del sistema

El menú **Registro de sucesos del sistema** permite ver y borrar los mensajes del registro de sucesos del sistema (SEL). Presione <Intro> para mostrar el **Menú del registro de sucesos 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 sucesos del sistema** y presione <Intro>. 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 sucesos del sistema** y presione <Intro>.

Cuando haya terminado con el menú del SEL, presione <Esc> para volver al menú anterior.

Salida de la utilidad de configuración del iDRAC6

Cuando haya terminado de hacer cambios en la configuración del iDRAC6, presione la tecla <Esc> para mostrar el menú de salida.

- Seleccione **Guardar cambios y salir** y presione <Intro> para retener los cambios. Si esta operación falla, aparece uno de los siguientes mensajes:
  - Falla de comunicación del iDRAC6: Aparece si el iDRAC no está accesible.
  - Algunos de los valores no se pueden aplicar: Aparece cuando algunos valores no se pueden aplicar.
- Seleccione **Descartar cambios y salir** y presione <Intro> para ignorar los cambios que ha realizado.
- Seleccione **Regresar a la configuración** y presione <Intro> para volver a la utilidad de configuración del iDRAC6.

18

Supervisión y administración de alertas

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 Managed System Software. 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 Microsoft Windows admitido con la función *Reiniciar automáticamente* de Windows deseleccionada en **Configuración de inicio y de recuperación de Windows**.
3. Active la pantalla de último bloqueo (desactivada de manera predeterminada).

   Para activarla por medio de RACADM local, abra un símbolo del sistema 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 basada en web del iDRAC6 funcione correctamente, desactive 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** a la izquierda.
3. Haga clic en la ficha **Advanced** (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 ficha **Advanced** (Opciones avanzadas).
3. En **Inicio y recuperación**, haga clic en **Configuración**.
4. Deseleccione la casilla de verificación **Reiniciar automáticamente**.
5. Haga clic dos veces en **Aceptar**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma tiene un mecanismo para configurar el dispositivo de acceso remoto para realizar las acciones seleccionadas ante ciertos mensajes de sucesos. Estas acciones incluyen reiniciar, ciclo de encendido, apagar y enviar una alerta (captura de sucesos de plataforma [PET] y/o por correo electrónico).

Los sucesos de plataforma que se pueden filtrar incluyen los siguientes:

1. Filtro de aserción de ventilador crítico
2. Filtro de aserción de advertencia de batería
3. Filtro de aserción de batería crítica
4. Filtro de aserción de voltaje crítico
5. Filtro de aserción de advertencia de temperatura
6. Filtro de aserción de temperatura crítica
7. Filtro de aserción de intromisión crítica
8. Filtro de redundancia degradada
9. Filtro de redundancia perdida
10. Filtro de aserción de advertencia de procesador
11. Filtro de aserción de procesador crítico
12. Filtro de aserción de advertencia de procesador
13. Filtro de aserción de advertencia de suministro de energía
14. Filtro de aserción de suministro de energía crítico
15. Filtro de aserción de suministro de energía ausente crítico
16. Filtro de aserción de registro de eventos crítico
17. Filtro de aserción de vigilancia crítica
18. Filtro de aserción de advertencia de alimentación del sistema
19. Filtro de aserción de alimentación del sistema crítica
20. Filtro de aserción informativa de medio flash extraíble ausente
21. Filtro de aserción de medio flash extraíble crítico
22. Filtro de aserción de advertencia de medio flash extraíble

Cuando se presenta un suceso de plataforma (por ejemplo, una falla de la sonda del ventilador), el suceso se genera y se registra en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) en la lista de los filtros de sucesos de plataforma y este filtro se ha configurado para que genere una alerta (PET o por correo electrónico), se envía una alerta de PET o por correo electrónico a un conjunto de uno o más destinos configurados.

Si el mismo filtro de sucesos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecuta.

Configuración de filtros de sucesos de plataforma (PEF)

Configure los filtros de sucesos de plataforma antes de configurar capturas de sucesos de plataforma o alertas por correo electrónico.

Configuración de PEF por medio de la interfaz web

Para obtener más información, ver "Configuración de filtros de sucesos de plataforma (PEF)" en la página 62.

Configuración de PEF por medio de la CLI de RACADM

1 Active el PEF.

Abra un símbolo del sistema, escriba el siguiente comando y presione <Intro>:

```
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 22. La selección de activación o desactivación puede ser 1 (activado) o 0 (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 el símbolo del sistema, escriba el comando siguiente y presione <Intro>:

```
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, ver "Configuración de capturas de sucesos de plataforma (PET)" en la página 63.

Configuración de PET por medio de la interfaz de línea de comandos de RACADM

1 Active las alertas globales.

Abra un símbolo del sistema, escriba el siguiente comando y presione <Intro>:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Active la PET.

En el símbolo del sistema, escriba los comandos siguientes y presione <Intro> después de cada uno:

```
IPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 1 1
```

```
IPv6: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:

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 4 1
```

3 Configure la política de PET.

En el símbolo del sistema, escriba el siguiente comando y presione <Intro>:

```
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 las direcciones IP de destino del sistema que recibe las alertas de sucesos de plataforma.

4 Configure la cadena de nombre de comunidad.

En el indicador 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, ver "Configuración de alertas por correo electrónico" en la página 64.

Configuración de alertas por correo electrónico por medio de la interfaz de línea de comandos de RACADM

1. Active las alertas globales.

   Abra un símbolo del sistema, escriba el siguiente comando y presione <Intro>:

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico.

   En el símbolo del sistema, escriba los siguientes comandos y presione <Intro> 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 el símbolo del sistema, escriba el siguiente comando y presione <Intro>:

```
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 sucesos de plataforma.

Para configurar un mensaje personalizado, en el símbolo del sistema escriba el comando siguiente y presione <Intro>:

```
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 suceso crítico en el sistema administrado. El ejemplo siguiente 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. Ver "Configuración de alertas por correo electrónico" en la página 353 para obtener más información.

Comprobación de la función de alertas de captura SNMP del RAC

La función de alertas de captura SNMP del RAC permite que las configuraciones del detector de capturas SNMP reciban las capturas 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 capturas SNMP del RAC.

```
racadm testtrap -i 2
```

Antes de probar la función de alertas de capturas SNMP del RAC, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Para configurar estos valores, consulte las descripciones de los subcomandos testtrap y testemail de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Preguntas frecuentes sobre la autentificación de SNMP

¿Por qué aparece el siguiente mensaje?

```
Acceso remoto: Fallo de autentificación 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 **public**. Cuando IT Assistant envía una solicitud Set, el agente iDRAC6 genera el error de autentificación SNMP porque sólo acepta solicitudes de **comunidad = public** (público).

NOTA: Este es el nombre de comunidad de agente SNMP.

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 mediante la interfaz web, diríjase a **Configuración→ Red/Seguridad→ Servicios** y haga clic en **Agente SNMP**.

Para evitar que se generen errores de autentificación 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.

19

Recuperación y solución de problemas del sistema administrado

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" en la página 357.
- "Administración de la alimentación en un sistema remoto" en la página 358.
- "Uso de los registros de inicio de la POST" en la página 368.
- "Visualización de la pantalla de último bloqueo del sistema" en la página 369.

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 inmovilizado?
3. Si está apagado, ¿se ha apagado de forma imprevista?

En el caso de un sistema bloqueado, revise la pantalla de último bloqueo (consulte "Visualización de la pantalla de último bloqueo del sistema" en la página 369) y use la consola virtual y la administración remota de la alimentación (consulte "Administración de la alimentación en un sistema remoto" en la página 358) para reiniciar el sistema y observar el proceso de reinicio.

Administración de la alimentación en un sistema remoto

El iDRAC6 permite realizar varias acciones de administración de la alimentación de forma remota en el sistema administrado para recuperarlo después de un bloqueo o de algún otro suceso del sistema.

Selección de las acciones de control de alimentación de la interfaz web del iDRAC6

Para realizar acciones de administración de la alimentación mediante la interfaz web, consulte "Ejecución de operaciones de control de alimentación en el servidor" en la página 328.

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 la alimentación 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 encenderlo.
- **powerstatus**: muestra el estado de alimentación actual del servidor ("Encendido" o "Apagado")
- **hardreset**: ejecuta una operación de restablecimiento (reinicio) en el sistema administrado.

Visualización de la información del sistema

La página **Resumen del sistema** le permite visualizar la condición del sistema y otra información básica del iDRAC6 y le proporciona vínculos de acceso a las páginas de condición e información del sistema. Además, desde esta página puede iniciar rápidamente tareas comunes y ver los sucesos recientes registrados en Registro de sucesos del sistema (SEL).

Para acceder a la página **Resumen del sistema**, haga clic en **Sistema**→ **Propiedades**→ ficha **Resumen del sistema**. Para obtener más información, consulte la *Ayuda en línea de iDRAC6*.

La página **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Chasis del sistema principal
- Remote Access Controller

Para tener acceso a la página **Resumen del sistema**, expanda el árbol **Sistema** y haga clic en **Propiedades**→ ficha **Detalles del sistema**.

Chasis del sistema principal

NOTA: Para recibir la información del **Nombre del host** y el **Nombre del sistema operativo**, debe tener instalados los servicios del iDRAC6 en el sistema administrado.

Tabla 19-1. Información del sistema

Campo	Descripción
Descripción	Descripción del sistema.
Versión del BIOS	Versión del BIOS del sistema.
Service Tag	Número de la etiqueta de servicio del sistema.
Código de servicio rápido	Código de servicio del sistema.
Host Name (Nombre de host)	Nombre del sistema host.
OS Name (Nombre del sistema operativo)	El sistema operativo que se ejecuta en el sistema.
OS versión (Versión del sistema operativo)	Versión del sistema operativo que se ejecuta en el sistema.
Revisión del sistema	Número de revisión del sistema.
Firmware de Lifecycle Controller	Versión de firmware de Lifecycle Controller.

Tabla 19-2. 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 ciclo de encendido.
Cuenta regresiva inicial	El número de segundos posteriores a la detección de un *sistema bloqueado* momento en el cual el iDRAC6 realizará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Tabla 19-3. Direcciones MAC del NIC incorporado

Campo	Descripción
MAC virtual	Muestra direcciones de control de acceso al medio virtual (MAC). Los datos de MAC virtual se obtienen del inventario de hardware, por lo que el inventario de hardware debe recopilarse antes de visualizar los datos de vMAC. Haga clic en **Inventario del sistema**. Se actualizan los datos de inventario y se muestran en la página **Inventario del sistema**. Haga clic otra vez en **Detalles del sistema**. Los MAC virtuales para cada uno de los puertos LAN incorporados se muestran en la página **Detalles del sistema**. **NOTA:** La función vMAC se usará por Dell Advanced Infrastructure Manager (AIM) en las siguientes publicaciones. Si Dell AIM no administra el servidor actualmente, entonces la dirección MAC de Ethernet y la dirección MAC virtual son identicas.

Tabla 19-3. Direcciones MAC del NIC incorporado *(continuación)*

Campo	Descripción
NIC 1	Muestra las direcciones de Ethernet, Interfaz estándar de equipos pequeños por Internet (iSCSI) y MAC virtual del controlador integrado de interfaces de red (NIC)1. Los NIC de Ethernet admiten el estándar de Ethernet cableado y enchufado en el bus del sistema del servidor. NIC iSCS es una controladora de interfaces de red con la pila de iSCSI que se ejectua en el equipo host. Las direcciones MAC identifican de forma particular cada nodo de una red en la capa de control de acceso al medio.
NIC 2	Muestra las direcciones de Ethernet, iSCSI y MAC virtual del controlador integrado de interfaces de red NIC 2 que lo identifican de manera exclusiva en la red.
NIC 3	Muestra las direcciones de Ethernet, iSCSI y MAC virtual del controlador integrado de interfaces de red NIC 3 que lo identifican de manera exclusiva en la red.
NIC 4	Muestra las direcciones de Ethernet, iSCSI y MAC virtual del controlador integrado de interfaces de red NIC 4 que lo identifican de manera exclusiva en la red.

Remote Access Controller

Tabla 19-4. Información del RAC

Campo	Descripción
Name (Nombre)	iDRAC6
Product Information	Integrated Dell Remote Access Controller 6 – Enterprise
Fecha/Hora	Tiempo actual en la forma: Día Mes DD HH:MM:SS AAAA Ejemplo: Vie 28 de enero 16:27:29 2011
Firmware Version (Versión de firmware)	Versión del firmware del iDRAC6

Tabla 19-4. Información del RAC *(continuación)*

Campo	Descripción
Firmware actualizado	Última fecha de actualización del firmware en la forma: Día Mes DD HH:MM:SS AAAA Ejemplo: Sáb 29 de enero de 2011, 13:31:50
Versión del hardware	Versión de Remote Access Controller
Dirección MAC	Muestra la dirección de control de acceso de medios (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red.

Tabla 19-5. Información IPv4

Campo	Descripción
IPv4 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.
predeterminada	Dirección de un enrutador o un conmutador. El valor se muestra en formato de números separados con puntos, por ejemplo, 143.166.154.1.
DHCP activado	**Sí** o **No.** Indica si el protocolo de configuración dinámica de host (DHCP) está activado.
Use DHCP para obtener direcciones del servidor DNS	**Sí** o **No.** Indica si se desea usar DHCP para obtener direcciones de servidor DNS.
Servidor DNS preferido	Indica la dirección IPv4 estática del servidor DNS preferido.
Servidor DNS alternativo	Indica la dirección IPv4 estática del servidor DNS alternativo.

Tabla 19-6. Campos de información IPv6

Campo	Descripción
IPv6 activado	Indica si la pila IPv6 está activada.
Dirección IP 1	Especifica el tamaño del prefijo/dirección IPv6 del NIC del iDRAC6. El *tamaño del prefijo* se combina con la dirección IP 1. Es un número entero que especifica el tamaño del prefijo de la dirección IPv6. Puede tener un valor entre 1 y 128 inclusive.
Puerta de enlace IP	Especifica la puerta de enlace del NIC del iDRAC6.
Dirección local de vínculo	Especifica la dirección IPv6 local del vínculo del NIC del iDRAC6.
Dirección IP 2...15	Especifica las direcciones IPv6 adicionales del NIC del iDRAC6, si están disponibles.
Configuración automática activada	**Sí** o **No.** AutoConfig permite que Server Administrator obtenga la dirección IPv6 para el NIC del iDRAC del servidor del protocolo de configuración dinámica de host (DHCPv6).
Usar DHCPv6 para obtener direcciones de servidor DNS	**Sí** o **No.** Indica si se desea usar DHCPv6 para obtener direcciones de servidor DNS.
Servidor DNS preferido	Indica la dirección IPv6 estática del servidor DNS preferido.
Servidor DNS alternativo	Indica la dirección IPv6 estática del servidor DNS alternativo.

Inventario del sistema

La página **Inventario del sistema** muestra información sobre los componentes de hardware y firmware instalados en el sistema.

Para tener acceso a la página **Inventario del sistema**, expanda el árbol **Sistema** y haga clic en **Propiedades→ System inventory**.

Inventario de hardware

Esta sección muestra información sobre los componentes de hardware presentes en el sistema. Si los datos de inventario de hardware no están disponibles cuando hace clic en la ficha **Inventario del sistema**, aparece el mensaje siguiente:

```
El inventario de hardware no está disponible.
```

Actualice la página para ver los detalles.

Inventario de firmware:

Esta sección muestra versiones de firmware de los componentes instalados de Dell. Si los datos de inventario de firmware no están disponibles cuando hace clic en la ficha **Inventario del sistema**, aparece el mensaje siguiente:

```
El inventario de hardware no está disponible.
```

Actualice la página para ver los detalles.

NOTA: Si CSIOR (Recopilación del inventario del sistema al reiniciar) no está activado, tarda algún tiempo en recopilar los datos, así que se recomienda ejecutar primero CSIOR y recopilar el inventario del sistema al reiniciarse, y luego hacer clic en la ficha **Inventario del sistema**.

Después de instalar o desinstalar nuevo hardware al sistema, puede que la página **Inventario del sistema** no actualice los cambios automáticamente. Esto se debe a que los datos del inventario recopilados durante el proceso de fabricación puede que no estén actualizados con los nuevos cambios.

Para resolver esto, durante la POST del BIOS seleccione la opción **Cntl+E** y active **Recopilar el inventario del sistema** al reiniciar el sistema. Guarde y salga de la opción **Cntl+E**.

El sistema se reinicia para recopilar el nuevo inventario del sistema. Cuando finaliza la recopilación del inventario, la página **Inventario del sistema** muestra los datos de inventario de hardware y software correctos.

Para obtener más información, consulte la *Ayuda en línea de iDRAC6*.

Uso del registro de sucesos del sistema (SEL)

La página **SEL** muestra los sucesos críticos del sistema que se presentan en el sistema administrado.

Para ver el registro de sucesos del sistema:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y después haga clic en **Registro de sucesos del sistema**.

   La página **Registro de sucesos del sistema** muestra la gravedad del suceso y ofrece otra información según se muestra en la Tabla 19-7.

3 Haga clic en el botón correspondiente de la página **Registro de sucesos del sistema** para continuar. Para obtener más información, consulte la Ayuda en línea de iDRAC6.

4 Haga clic en **Borrar registro** para borrar el SEL.

NOTA: El botón Borrar registro sólo aparece si tiene permiso para Borrar registros.

5 Haga clic en **Guardar como** para guardar el registro de sucesos del sistema en el directorio de su elección.

Tabla 19-7. Iconos de indicador de estado

Icono/categoría	Descripción
	Una marca de verificación verde indica una condición de estado satisfactoria (normal).
	Un triángulo amarillo que contiene un signo de exclamación 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 suceso. Si la fecha está en blanco, el suceso se presentó durante el inicio del sistema. El formato es <día> <mes> dd aaaa hh:mm:ss, según el horario de 24 horas.
Descripción	Una breve descripción del suceso.

Activación/ desactivación de los registros de sucesos OEM

Los registros de sucesos OEM se muestran en la página **Registro de sucesos del sistema** automáticamente. El botón **Configuración avanzada** de la ficha **Sistema→ Registros** permite activar o desactivar los mensajes de sucesos OEM del sistema administrado que aparecen en la página **Registro de sucesos del sistema**.

Para que los registros de sucesos OEM no aparezcan en la página **Registro de sucesos del sistema**, seleccione la opción **Filtrado de eventos OEM y SEL activado**.

NOTA: La opción **Filtrado de eventos OEM y SEL activado** no está seleccionada por defecto.

Uso de la línea de comandos para ver el registro del sistema

```
racadm getsel -i
```

El comando **getsel -i** muestra el número de anotaciones en SEL.

```
racadm getsel <opciones>
```

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

NOTA: Para obtener más información sobre las opciones que puede utilizar, consulte el subcomando getsel de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support **dell.com/support/manuals**.

El comando **clrsel** elimina todos los registros existentes del SEL.

```
racadm clrsel
```

Uso de las notas de trabajo

Las notas de trabajo son notas o comentarios que un usuario puede añadir. Cualquier usuario iDRAC puede añadir una nota de trabajo. Las notas de trabajo no se pueden eliminar. Puede visualizar hasta 1000 notas de trabajo a la vez. Para una referencia rápida, las últimas diez notas de trabajo se muestran en la página de inicio del iDRAC.

NOTA: Si el número de notas de trabajo añadidas son más de 800, la página de la interfaz gráfica de usuario puede tardar unos segundos en cargar la página. Esto se debe a la transacción entre la interfaz gráfica de usuario y el iDRAC6 de una cantidad relativamente grande de datos. Puede que las notas de trabajo que se acaban de añadir no se muestren una vez se haya cargado la página. Para resolver este problema, haga clic en **Actualizar**.

La página **Notas de trabajo** le permite introducir notas de trabajo en Lifecycle Log. La fecha y la hora de la nota se registran automáticamente.

Para acceder a la página **Notas de trabajo**, expanda el árbol del **Sistema** y haga clic en **Sistema→ Registros→ Notas de trabajo**.

Aparece la página **Notas de trabajo** que le permite introducir notas de trabajo y le proporciona otra información como se muestra en Tabla 19-8.

Para introducir las notas de trabajo:

1 En la página **Notas de trabajo**, en la sección **Añadir notas de trabajo**, introduzca la nota de trabajo en el campo que aparece.

NOTA: Se admite un máximo de 50 caracteres alfanuméricos en la nota de trabajo.

2 Haga clic en **Save** (Guardar).

La nueva nota de trabajo se muestra en la tabla de notas de trabajo debajo de la sección **Añadir notas de trabajo**.

Tabla 19-8. Notas de trabajo

Campo	Descripción
Fecha/Hora	Muestra la fecha y la hora registrada para cada entrada de nota de trabajo. El formato es aaaa-mm-ddHhh:mm:ssZ, según el horario de 24 horas, en que, aaaa : año mm : mes dd : día H : hora hh : hora mm : minuto ss : segundos Z : designa la zona horaria. **NOTA:** Si la hora está en formato UTC, añada una **Z** justo después de la hora sin dejar espacio. **Z** designa la zona si la diferencia UTC es cero. **09:30** UTC se representa por lo tanto como **09:30Z** o **0930Z**. **14:45:15** UTC sería **14:45:15Z** o **144515Z**.
Notes (Notas)	Muestra el contenido de la entrada de la nota de trabajo.

Uso de los registros de inicio de la POST

NOTA: Todos los registros se borran después de reiniciar el iDRAC6.

La página **Captura de inicio** brinda acceso a los registros de hasta los últimos tres ciclos de inicio disponibles. Están ordenados del más reciente al más antiguo. Si el servidor no ha atravesado ningún ciclo de inicio, se muestra **No hay registros disponibles**. Haga clic en **Reproducir** después de seleccionar un ciclo de inicio disponible para mostrarlo en una ventana nueva.

NOTA: La visualización de la captura de inicio sólo se admite en Java y no se admite en Active-X.

Para ver los registros de capturas de inicio:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y luego en la ficha **Captura de inicio**.
3. Seleccione un ciclo de inicio y haga clic en **Reproducir**.

   El vídeo de los registros se reproduce en una nueva pantalla.

   NOTA: Debe cerrar el vídeo abierto de registro de captura de inicio antes de reproducir otro. No se pueden reproducir dos registros simultáneamente.
4. Haga clic en **Reproducción→ Reproducir** para comenzar el vídeo de registro de captura de inicio.
5. Haga clic en **Reproducción→ Controles de medios** para detener el vídeo.

NOTA: Puede aparecer un mensaje solicitando que guarde un archivo **data.jnlp** en lugar de abrir el visor. Para resolver este problema, realice el siguiente procedimiento en Internet Explorer: Vaya a **Herramientas→ Opciones de Internet→** ficha **Opciones avanzadas** y deseleccione la opción *No guardar las páginas cifradas en el disco.*

NOTA: Si el iDRAC se restablece, el vídeo de captura de inicio no está disponible ya que está almacenado en la memoria RAM y se elimina cuando el iDRAC se restablece.

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 SEL y la pantalla LCD: `Actualización satisfactoria del iDRAC6`. Si falla, se registra el siguiente mensaje: `Falló la actualización del iDRAC6`. Aun más, cuando una tarjeta iDRAC6 Express con el firmware de un 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: `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 Lifecycle Controller*.

Visualización de 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 ficha **Red/Seguridad** en la sección **Configuración del iDRAC** para activar esta función.

Para ver la página **Pantalla de último bloqueo**:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y luego en **Pantalla** de **último bloqueo**.

   La página **Pantalla de último bloqueo** muestra la pantalla del bloqueo del sistema más reciente. La información del último bloqueo se guarda en la memoria del iDRAC6 y se puede acceder a ella de manera remota.

   Para obtener más información sobre los botones que aparecen en la página **Pantalla de último bloqueo** consulte la *ayuda en línea del iDRAC6*.

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 menor a 30 segundos. Utilice Server Administrator o IT Assistant para establecer el valor del temporizador de restablecimiento del sistema en no menos de 30 segundos y compruebe que la **Pantalla de último bloqueo** funcione correctamente. Ver "Configuración del sistema administrado para capturar la pantalla de último bloqueo" en la página 347 para obtener más información.

20

Recuperación y solución de problemas del iDRAC6

Esta sección explica cómo realizar las tareas relacionadas con la recuperación y solución de problemas de un iDRAC6 bloqueado.

Se puede usar una de las siguientes herramientas para solucionar problemas en el iDRAC6.

- Registro del RAC
- Consola de diagnósticos
- Identificar servidor
- 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 de sesión y desconexión, y cambios en las políticas de seguridad) y de alertas generadas por el iDRAC6. Cuando el registro se llena, las anotaciones más antiguas se sobrescriben.

Para acceder al registro del RAC desde la interfaz de usuario del iDRAC6:

1. En el árbol del **Sistema**, haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Registros** y luego en **Registro del iDRAC**.

La página **Registro del iDRAC** muestra la información que aparece en la Tabla 20-1.

Tabla 20-1. Información de la página Registro del iDRAC

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, `19 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 `Inicio del sistema`.
Origen	La interfaz que ocasionó el suceso.
Descripción	Una breve descripción del suceso y el nombre de usuario que inició sesión en el iDRAC6.

NOTA: Para obtener información sobre el uso de los botones de la página **Registro del iDRAC**, consulte la *Ayuda en línea del iDRAC6*.

Uso de la línea de comandos

Utilice el comando `getraclog` para ver las anotaciones del registro del iDRAC6.

```
racadm getraclog [opciones]
```

```
racadm getraclog -i
```

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

NOTA: Para obtener más información, consulte getraclog en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Se puede usar el comando `clrraclog` para borrar todas las anotaciones del registro del iDRAC.

```
racadm clrraclog
```

Uso de la consola de diagnósticos

El iDRAC6 proporciona un conjunto estándar de herramientas de diagnóstico de red (ver Tabla 20-2) que son similares a las herramientas que se incluyen en los sistemas con Microsoft Windows o Linux. Por medio de la interfaz basada en web del iDRAC6 se puede acceder a las herramientas de depuración de red.

Haga clic en **Restablecer iDRAC6** para restablecer el iDRAC. Se realiza una operación de inicio normal en el iDRAC.

Para acceder a la página de **Consola de diagnósticos**:

1. En el árbol **Sistema**, haga clic en **Configuración del iDRAC**→ ficha **Solución de problemas**→ **Consola de diagnósticos**.
2. Escriba un comando y haga clic en **Enviar**. En la Tabla 20-2 se describen los comandos que se pueden utilizar. Los resultados de la depuración aparecen en la página **Consola de diagnósticos**.
3. 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 20-2. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las anotaciones 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 enrutamiento. Si se proporciona el número de interfaz opcional en el campo de texto situado a la derecha de la opción **netstat**, dicha opción imprime información adicional acerca del tráfico por la interfaz, uso del búfer y otra información de la 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 enrutamiento. Se debe introducir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco del protocolo de mensajes de control de Internet (ICMP) se envía a la dirección IP de destino en base al contenido de la tabla de enrutamiento actual.

Tabla 20-2. Comandos de diagnóstico *(continuación)*

Comando	Descripción
gettracelog	Muestra el registro de rastreo del iDRAC6. Para obtener más información, consulte gettracelog en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Uso de la función de identificación de servidor

La página **Identificar** permite activar la función de identificación del sistema.

Para identificar el servidor:

1. Haga clic en **Sistema→ Configuración del iDRAC→ Solución de problemas→ Identificar**.
2. En la pantalla **Identificar**, seleccione la casilla de marcación **Identificar servidor** para activar el parpadeo de la pantalla LCD y el indicador LED de identificación en la parte posterior del servidor.
3. El campo **Tiempo de espera para identificar el servidor** muestra la cantidad de segundos que la pantalla LCD parpadea. Introduzca la cantidad de tiempo (en segundos) que desea que parpadee la pantalla LCD. El rango del tiempo de espera es de 1 a 255 segundos, inclusive. Si el tiempo de espera se define en 0, la pantalla LCD parpadea continuamente.
4. Haga clic en **Aplicar**.

Si introdujo **0** segundos, siga estos pasos para desactivarlo:

1. Haga clic en **Sistema→ Configuración del iDRAC→ Solución de problemas→ Identificar**.
2. En la pantalla **Identificar**, deseleccione la opción **Identificar servidor** y haga clic en **Aplicar**.

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 del **Sistema**, haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **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 en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

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 genera un eco para un ICMP (ping) con un tamaño de paquete mayor de 1500 bytes.

Uso de racdump

El comando `racadm racdump` proporciona un solo comando para obtener información sobre volcado, estado e información general sobre la tarjeta del iDRAC6

NOTA: Este comando está disponible sólo en Telnet, SSH e interfaces remotas de racadm. Para obtener más información, consulte el comando racdump en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Uso de coredump

El comando `racadm coredump` muestra información detallada sobre cualquier problema crítico reciente que se ha 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 persiste después de ciclos de encendido del RAC y sigue disponible hasta que se presenta una 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. Para obtener más información, consulte los subcomandos `coredump` y `coredumpdelete` en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

21

Sensores

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 usarse para supervisar los sensores de hardware en baterías, sondas de ventilador, intromisión en el chasis, fuentes de alimentación, consumo de energía, temperatura y voltajes.

Sondas de baterías

Las sondas de baterías proporcionan 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 las 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 intromisión en el chasis

Las sondas de intromisión en el chasis indican el estado del chasis, si está abierto o cerrado.

Sondas de fuentes de alimentación

Las sondas de fuentes de alimentación proporcionan la siguiente información:

- Estado de las fuentes de alimentación
- Redundancia de la fuente de alimentación, es decir, la capacidad de la fuente de alimentación redundante de reemplazar a la fuente de alimentación principal si ésta falla.

NOTA: Si sólo existe una fuente de alimentación en el sistema, la redundancia de la fuente de alimentación estará **desactivada.**

Sondas de medios flash extraíbles

El sensor de medios flash extraíbles proporciona información acerca del estado de la tarjeta vFlash SD (activa o ausente). Para obtener más información acerca de la tarjeta vFlash SD, ver "Configuración de la tarjeta vFlash SD y administración de las particiones vFlash" en la página 299.

Sondas de supervisión de la alimentación

La supervisión de la alimentación proporciona 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 proporciona 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 estas 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.

22

Configuración de las funciones de seguridad

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Opciones de seguridad avanzada para el administrador del iDRAC6:
  - La opción de desactivación de la consola virtual le permite al usuario del sistema *local* desactivar la consola virtual utilizando la función Consola virtual 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 utiliza el 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 del tiempo de espera de la sesión (en segundos) mediante la interfaz web o la interfaz de línea de comandos de RACADM
- Puertos IP que se pueden configurar (si corresponde)
- Secure Shell (SSH), que usa una capa de transporte cifrado para ofrecer mayor seguridad
- Límites de fallo de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando se 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

Desactivación de la configuración local del iDRAC6

Los administradores pueden desactivar la configuración local por medio de la interfaz gráfica de usuario del iDRAC6 al seleccionar **Configuración del iDRAC→ Red/Seguridad→ 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 mediante la interfaz basada en web.

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 a esta versión, deberá actualizar el BIOS. Actualice el BIOS mediante el paquete de actualización del BIOS desde el sitio web del servicio de asistencia Dell Support 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 usando 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. Se recomienda utilizar estas funciones con moderación. Desactive sólo una interfaz a la vez para evitar perder todos los privilegios de acceso.

NOTA: Para obtener más información, consulte el documento técnico *Disabling Local Configuration and Remote Virtual KVM in the DRAC* (Desactivación de la configuración local y el KVM virtual remoto en el DRAC) en el sitio web del servicio de asistencia Dell Support 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 los servidores no necesiten tener acceso administrativo a los dispositivos de acceso remoto. Asimismo, los técnicos pueden tener acceso físico a los servidores durante el mantenimiento de rutina de los 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 deben 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 desactivado 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 autentificación de Active Directory, es posible que los administradores no puedan iniciar sesión. De la misma forma, 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 dinámica de host (DHCP), y el servidor DHCP asigna entonces la dirección IP del iDRAC6 a otro dispositivo de la red, el conflicto resultante podría ocasionar la desactivación de la conectividad fuera de banda del DRAC, lo que obligaría a los administradores a restablecer la configuración predeterminada del firmware por medio de una conexión serie.

Desactivación de la consola virtual del iDRAC6

Los administradores pueden desactivar la consola virtual del iDRAC6 de manera selectiva, lo que proporciona 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 consola virtual. El uso de esta función requiere la instalación en el servidor del software de nodo administrado del iDRAC. Los administradores pueden desactivar la consola virtual con el siguiente comando:

```
racadm LocalConRedirDisable 1
```

El comando LocalConRedirDisable desactiva las ventanas de sesión de la consola virtual 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 la consola virtual. Pueden hacer esto con el argumento 0:

```
racadm LocalConRedirDisable 0
```

Hay varias situaciones que pueden requerir la desactivación de la consola virtual 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 cuyo caso pueden desactivar la consola virtual durante la POST del sistema por medio del comando `LocalConRedirDisable`. Si también desean aumentar la seguridad mediante la desactivación automática de la consola virtual cada vez que un administrador inicia sesión en el sistema, lo pueden hacer ejecutando el comando `LocalConRedirDisable` en las secuencias de comandos de inicio de sesión del usuario.

NOTA: Para obtener más información, consulte el documento técnico *Disabling Local Configuration and Remote Virtual KVM in the DRAC* (Desactivación de la configuración local y el KVM virtual remoto en el DRAC) en el sitio web del servicio de asistencia Dell Support 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)

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 autentificada entre los clientes y servidores a fin de evitar intercepción furtiva a la información de la red.

Un sistema habilitado para SSL:

- Se autentifica a sí mismo en un cliente habilitado para SSL
- Permite que el cliente se autentifique a sí mismo en el servidor
- Permite que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado proporciona una protección de datos de alto nivel. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado disponible en general 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:

1. Sustituya el certificado SSL del servidor web por un certificado válido de una autoridad de certificados (CA, por sus siglas en inglés).
2. Genere una solicitud de firma de certificado (CSR, por sus siglas en inglés) mediante el envío de una solicitud al iDRAC6.
3. Proporcione el CSR a la autoridad de certificados (CA) para obtener un certificado válido.

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 CA y se cargue el certificado devuelto por la CA.

Una CA 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 autoridades de certificados se incluyen Thawte y VeriSign. Después de recibir la solicitud CSR, la CA revisa y verifica la información que contiene la CSR. 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 Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.

2 Haga clic en la ficha **Red/Seguridad** y luego en **SSL**.

Utilice el **Menú Principal de SSL** consulte la Tabla 22-1) 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. Para obtener información sobre los botones disponibles en la página **SSL**, consulte la *Ayuda en línea del iDRAC6*.

Tabla 22-1. 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.

Generación de una solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribe la CSR anterior en el firmware. Antes de que iDRAC pueda aceptar un certificado firmado, la CSR en el firmware debe coincidir con el certificado que CA devuelva.

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 22-2 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. Para obtener más información sobre los botones disponibles en la página **Generar solicitud de firma de certificado (CSR)** consulte la *Ayuda en línea del iDRAC6*.

Tabla 22-2. 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, **xyzcompany.com**). Son válidos los caracteres alfanuméricos, guiones y puntos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Son válidos los caracteres alfanuméricos, guiones y puntos.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Grupo de servidores empresariales). Son válidos los caracteres alfanuméricos, guiones y puntos.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Son válidos los caracteres alfanuméricos, guiones y puntos.
Nombre del estado	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Texas). Son válidos los caracteres alfanuméricos, guiones y puntos.
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.

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 22-3 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 del servidor** para continuar.

Tabla 22-3. Información de certificados

Campo	Descripción
Serial Number (Número de serie)	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el titular
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, ver "Uso de Secure Shell (SSH)" en la página 97.

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 Expanda el árbol del **Sistema** y haga clic en **Configuración del iDRAC**.

2 Haga clic en la ficha **Red/Seguridad** y luego en **Servicios**.

3 Configure los servicios siguientes según sea necesario:

- Configuración local (Tabla 22-4)
- Web Server (Tabla 22-5)
- SSH (Tabla 22-6)

- Telnet (Tabla 22-7)
- RACADM remoto (Tabla 22-8)
- Agente SNMP (Tabla 22-9)
- Agente de recuperación automática del sistema (Tabla 22-10)

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 definiendo la **Acción** ya sea 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** para aplicar los valores de la página Servicios.

Tabla 22-4. 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 pide que introduzca el módulo de configuración con la combinación de teclas <Ctrl+E> durante el reinicio del sistema.
Desactivación de la configuración local del iDRAC por medio de RACADM	Desactiva la configuración local del iDRAC por medio de RACADM local.

Tabla 22-5. Configuración del servidor Web

Valor	Descripción
Activado	Activa o desactiva el servidor web. Seleccionado=activado; deseleccionado=desactivado.
N.º 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**.

Tabla 22-5. Configuración del servidor Web *(continuación)*

Valor	Descripción
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cancela cuando se agota el tiempo de espera. Los cambios a la configuración del tiempo de espera actúan de inmediato y terminan la sesión de interfaz web actual. El servidor web también se restablecerá. Espere unos minutos antes de abrir una nueva sesión de interfaz web. El rango del tiempo de espera 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 22-6. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando se selecciona, SSH está activado.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango de tiempo de espera es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es 300.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es 22.

Tabla 22-7. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, SSH está activado.
Tiempo de espera	El tiempo de espera en inactividad de Telnet, en segundos. El rango de tiempo de espera es de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es 300.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es 23.

Tabla 22-8. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Si está seleccionado, la RACADM remota está activada.
Sesiones activas	El número de sesiones actuales en el sistema.

Tabla 22-9. Configuración del agente SNMP

Valor	Descripción
Activado	Activa o desactiva el agente SNMP. Seleccionado=activado; deseleccionado=desactivado.
Nombre de comunidad	Define la cadena de comunidad de SNMP que vaya a utilizar. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 22-10. Configuración del agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automática del sistema.

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 correspondientes valores de tiempo de espera 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 trabajo 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 concede acceso al iDRAC6 Los inicios de sesión provenientes de direcciones IP fuera de este rango reciben un mensaje de error.

El inicio de sesión prosigue 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 la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para ver una lista completa de las propiedades de **cfgRacTuning**.

Tabla 22-11. 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 permite establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que están fuera de este rango fallan. Los valores predeterminados de 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.
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

Vea el siguiente comando de ejemplo para la configuración del filtrado de IP.

Ver "Uso de RACADM de manera remota" en la página 120 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 en la siguiente sección:

```
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 en la siguiente sección:

```
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 siguientes al activar 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 de 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, éstos 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, ciertos clientes de SSH pueden mostrar el siguiente mensaje: `Identificación de intercambio de SSH: El host remoto cerró la conexión.`

Consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para ver una lista completa de las propiedades de **cfgRacTuning**.

La Tabla 22-12 muestra una lista de los parámetros definidos por el usuario.

Tabla 22-12. 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 siguiente impide que una dirección IP cliente establezca una sesión durante cinco minutos si 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 impide más de tres intentos fallidos dentro de un minuto e impide 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 la red por medio de la interfaz gráfica de usuario del iDRAC6

NOTA: Para poder realizar los pasos que siguen, se debe tener permiso para Configurar el iDRAC6

1. En el árbol del **Sistema**, haga clic en **Configuración del iDRAC**.
2. Haga clic en la ficha **Red/Seguridad** y luego haga clic en **Red**.
3. En la página **Configuración de la red**, haga clic en **Configuración avanzada**.
4. En la página **Seguridad de la red**, configure los valores de los atributos y luego haga clic en **Aplicar cambios**.

   La Tabla 22-13 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**. Para obtener más información sobre los botones de la página **Seguridad de la red**, consulte la *Ayuda en línea de iDRAC6*.

Tabla 22-13. valores de la página de seguridad de la red

Valor	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 el operador Y con la máscara de subred de 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 permite establecer una sesión en el iDRAC6. Los inicios de sesión provenientes de direcciones IP que están fuera de este rango fallan. Los valores predeterminados de 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 fallas de 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 fallas de bloqueo de IP	Determina el plazo en segundos durante el cual deben ocurrir el número de errores por fallos de bloque de IP 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.

Índice

A

B

C

K

L

M

O

P

R

S

T

U

V