Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 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.

Marzo 2009 Rev. A00

Regresar a la página de contenido

Generalidades del subcomando RACADM

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

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

---

help

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

Tabla A-1. Comando help

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

Sinopsis

```
racadm help

racadm help <subcomando>
```

Descripción

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

Salida

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

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

Interfaces admitidas

- RACADM local

---

config

Tabla A-2 describe los subcomandos **config** y **getconfig**.

Tabla A-2. config/getconfig

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

Sinopsis

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

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

Interfaces admitidas

- RACADM local

Descripción

El subcomando **config** permite establecer parámetros de configuración de iDRAC individualmente o procesarlos en lote como parte de un archivo de configuración. Si la información es diferente, ese objeto de iDRAC se escribirá con el nuevo valor.

Entrada

En la tabla A-3 se describen las opciones del subcomando **config**.

Tabla A-3. Opciones y descripciones del subcomando config

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

Salida

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

- Sintaxis, nombre de grupo, nombre de objeto o índice no válidos, u otros miembros no válidos de la base de datos
- Fallas de la CLI de RACADM

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

Ejemplos

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110`

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

- `racadm config -f myrac.cfg`

  Configura o reconfigura el iDRAC. El archivo **myrac.cfg** se puede crear con el comando **getconfig**. El archivo **myrac.cfg** también se puede editar manualmente siempre y cuando se sigan las reglas de análisis.

  NOTA: El archivo **myrac.cfg** no contiene contraseñas. Para incluir contraseñas en el archivo, usted debe introducirlas manualmente. Si desea eliminar contraseñas del archivo **myrac.cfg** durante la configuración, use la opción **-p**.

getconfig

El subcomando **getconfig** permite recuperar parámetros de configuración de iDRAC individualmente o se pueden recuperar todos los grupos de configuración de iDRAC y guardarse en un archivo.

Entrada

En la tabla A-4 se describen las opciones del subcomando **getconfig**.

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

Tabla A-4. Opciones del subcomando getconfig

Opción	Descripción
-f	La opción **-f** <*nombre_de_archivo*> redirige **getconfig** para que escriba toda la configuración de iDRAC en un archivo de configuración. Este archivo se puede usar entonces para realizar operaciones de configuración de procesamiento en lote por medio del subcomando **config**. **NOTA:** La opción **-f** no crea anotaciones para los grupos **cfgIpmiPet** y **cfgIpmiPef**. Usted debe establecer al menos un destino de captura para capturar el grupo **cfgIpmiPet** en el archivo.
-g	La opción **-g** <*nombre_de_grupo*>, o de grupo, se puede usar para mostrar la configuración de un solo grupo. El *nombre_de_grupo* es el nombre del grupo que se utiliza en los archivos **racadm.cfg**. Si el grupo es un grupo indexado, use la opción **-i**.
-h	La opción **-h**, o de ayuda, muestra una lista de todos los grupos de configuración disponibles que se pueden usar. Esta opción es útil cuando usted no recuerda los nombres exactos de los grupos.
-i	La opción **-i** <*índice*>, o de índice, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. Si **-i** <*índice*> no se especifica, se asumirá un valor de 1 para los grupos, que son tablas que tienen varias anotaciones. El índice se especifica mediante el valor del índice; no mediante un valor asignado.
-o	La opción -o <*nombre_de_objeto*>, o de objeto, especifica el nombre de objeto que se usa en la consulta. Esta opción se puede usar con la opción **-g**.
-u	La opción **-u** <*nombre_de_usuario*>, o de nombre de usuario, se puede usar para mostrar la configuración del usuario especificado. La opción <***nombre_de_usuario***> es el nombre de usuario para inicio de sesión.
-v	La opción **-v**, o detallada, muestra detalles adicionales en propiedades y se utiliza con la opción **-g**.

Salida

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

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

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

Ejemplos

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

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

- `racadm getconfig -h`

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

- `racadm getconfig -u root`

  Muestra las propiedades de configuración del usuario **root**.

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

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

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>

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

racadm getconfig -u <nombre_de_usuario>

racadm getconfig -h
```

Interfaces admitidas

- RACADM local

---

getssninfo

En la tabla A-5 se describe el subcomando **getssninfo**.

Tabla A-5. Subcomando getssninfo

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

Sinopsis

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

Descripción

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

- Nombre de usuario
- Dirección IP (si corresponde)
- Tipo de sesión (por ejemplo, SSH o Telnet)
- Consolas en uso (por ejemplo, Medios virtuales o KVM virtual)

Interfaces admitidas

- RACADM local

Entrada

En la tabla A-6 se describen las opciones del subcomando **getssninfo**.

Tabla A-6. Opciones del subcomando getssninfo

Opción	Descripción
-A	La opción **-A** elimina la impresión de los encabezados de los datos.
-u	La opción de nombre de usuario **-u** <*nombre_de_usuario*> limita la salida impresa a sólo registros detallados de la sesión para el nombre de usuario determinado. Si se proporciona un asterisco (*) como nombre de usuario, aparecerá una lista de todos los usuarios. La información de resumen no aparecerá cuando se especifique esta opción.

Ejemplos

- `racadm getssninfo`

La tabla A-7 ofrece un ejemplo del mensaje de salida del comando **racadm getssninfo**.

Tabla A-7. Ejemplo del mensaje de salida del subcomando getssninfo

Usuario	Dirección IP	Tipo	Consolas
root	192.168.0.10	Telnet	KVM virtual

- racadm getssninfo -A

  "root" 143.166.174.19 "Telnet" "NINGUNO"

- racadm getssninfo -A -u *

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

- "bob" "143.166.174.19" "GUI" "NINGUNO"

---

getsysinfo

En la tabla A-8 se describe el subcomando **racadm getsysinfo**.

Tabla A-8. getsysinfo

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

Sinopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

Descripción

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

Interfaces admitidas

- RACADM local

Entrada

En la tabla A-9 se describen las opciones del subcomando **getsysinfo**.

Tabla A-9. Opciones del subcomando getsysinfo

Opción	Descripción
-d	Muestra la información de iDRAC.
-s	Muestra la información del sistema
-w	Muestra la información de vigilancia
-A	Elimina la impresión de encabezados/etiquetas.

Salida

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

Ejemplo del mensaje de salida

```
RAC Information:
RAC Date/Time           = Wed Aug 22 20:01:33 2007
```

```
Firmware Version         = 0.32
Firmware Build           = 13661
Last Firmware Update     = Mon Aug 20 08:09:36 2007

Hardware Version         = NA
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 1
MAC Address              = 00:14:22:18:cd:f9
Current DNS Server 1     = 10.32.60.4
Current DNS Server 2     = 10.32.60.5
DNS Servers from DHCP    = 1
Register DNS RAC Name    = 1
DNS RAC Name             = iDRAC-783932693338
Current DNS Domain       = us.dell.com

System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status             = OFF

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

Ejemplos

- `racadm getsysinfo -A -s`

  `"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"`

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status            = ON


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

Restricciones

Los campos **nombre de host** y **nombre de sistema operativo** en el mensaje de **getsysinfo** muestran la información correcta sólo cuando Dell OpenManage está instalado en el servidor administrado. Si OpenManage no está instalado en el servidor administrado, es posible que estos campos aparezcan en blanco o muestren información incorrecta.

---

getractime

En la tabla A-10 se describe el subcomando **getractime**.

Tabla A-10. getractime

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

Sinopsis

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

Descripción

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

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

Salida

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

Ejemplo del mensaje de salida

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

Interfaces admitidas

- RACADM local

---

setniccfg

En la tabla A-11 se describe el subcomando **setniccfg**.

Tabla A-11. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

Sinopsis

```
racadm setniccfg -d

racadm setniccfg -s [<dirección_IP> <máscara_de_red> <puerta_de_enlace>]

racadm setniccfg -o [<dirección_IP> <máscara_de_red> <puerta_de_enlace>]
```

Descripción

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

- La opción **-d** activa DHCP para el NIC (el valor predeterminado es DHCP activado).
- La opción **-s** activa la configuración de IP estática. Se pueden especificar la dirección IP, la máscara de red y la puerta de enlace. De lo contrario, se usa la configuración estática existente. <*dirección_IP*>, <*máscara_de_red*> y <*puerta_de_enlace*> se deben escribir como cadenas separadas con puntos.

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
  ```

- La opción **-o** desactiva el NIC completamente. <*dirección_IP*>, <*máscara_de_red*> y <*puerta_de_enlace*> se deben escribir como cadenas separadas con puntos.

  ```
  racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
  ```

Salida

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

Interfaces admitidas

- RACADM local

---

getniccfg

En la tabla A-12 se describe el subcomando **getniccfg**.

Tabla A-12. getniccfg

Subcomando	Definición
getniccfg	Muestra la configuración IP actual del iDRAC.

Sinopsis

```
racadm getniccfg
```

Descripción

El subcomando **getniccfg** muestra la configuración actual de la tarjeta de interfaz de red.

Ejemplo del mensaje de salida

Si la operación no es satisfactoria, el subcomando **getniccfg** muestra el mensaje de error correspondiente. De lo contrario, cuando se ejecute satisfactoriamente, el mensaje aparecerá en el formato siguiente:

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces admitidas

- RACADM local

---

getsvctag

En la tabla A-13 se describe el subcomando **getsvctag**.

Tabla A-13. getsvctag

Subcomando	Definición
getsvctag	Muestra la etiqueta de servicio.

Sinopsis

```
racadm getsvctag
```

Descripción

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

Ejemplo

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

```
Y76TP0G
```

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

Interfaces admitidas

- RACADM local

---

racreset

En la tabla A-14 se describe el subcomando **racreset**.

Tabla A-14. racreset

Subcomando	Definición
racreset	Restablece el iDRAC.

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

Sinopsis

```
racadm racreset
```

Descripción

El subcomando **racreset** realiza un restablecimiento de iDRAC. El suceso de restablecimiento se escribe en el registro de iDRAC.

Ejemplos

- `racadm racreset`

  Inicia la secuencia de restablecimiento ordenado de iDRAC.

Interfaces admitidas

- RACADM local

---

racresetcfg

En la tabla A-15 se describe el subcomando **racresetcfg**.

Tabla A-15. racresetcfg

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

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- RACADM local

Descripción

El comando **racresetcfg** elimina todas las anotaciones de la propiedad de base de datos configuradas por el usuario. La base de datos tiene propiedades predeterminadas para todas las anotaciones que se usan para restablecer los valores predeterminados originales del iDRAC.

AVISO: Este comando elimina la configuración actual del iDRAC y restablece la configuración predeterminada del mismo. Después del restablecimiento, el nombre y la contraseña predeterminados son **root** y **calvin**, respectivamente, y la dirección IP es **192.168.0.120** más el número de la ranura en la que se encuentra el servidor en el chasis.

---

serveraction

En la tabla A-16 se describe el subcomando **serveraction**.

Tabla A-16. serveraction

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

Sinopsis

```
racadm serveraction <acción>
```

Descripción

El subcomando **serveraction** permite que los usuarios realicen operaciones de administración de la alimentación en el sistema host. En la tabla A-17 se describen las opciones de control de alimentación de **serveraction**.

Tabla A-17. Opciones del subcomando serveraction

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

Salida

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

Interfaces admitidas

- RACADM local

---

getraclog

En la tabla A-18 se describe el comando **racadm getraclog**.

Tabla A-18. getraclog

Comando	Definición
getraclog -i	Muestra el número de anotaciones en el registro de iDRAC.
getraclog	Muestra las anotaciones del registro de iDRAC.

Sinopsis

```
racadm getraclog -i

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

Descripción

El comando **getraclog -i** muestra el número de anotaciones en el registro de iDRAC.

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

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

Tabla A-19. Opciones del subcomando getraclog

Opción	Descripción
-A	Muestra el mensaje de salida sin encabezados ni etiquetas.
-c	Proporciona la cuenta máxima de anotaciones a generar.
-m	Muestra una pantalla de información a la vez y pide al usuario que continúe (es parecida al comando **more** de UNIX).
-o	Muestra el mensaje de salida en una sola línea.
-s	Especifica la anotación inicial a partir de la cual se muestra la información.

Salida

El mensaje de salida predeterminado muestra el número de anotación, la fecha y la hora, el origen y la descripción. La fecha y hora comienza a la media noche del 1º de enero y avanza hasta que el servidor administrado se inicia. Después de que el servidor administrado se inicia, la hora de sistema del mismo se usa para registrar la fecha y hora.

Ejemplo del mensaje de salida

```
Record:       1
Date/Time:    Dec 8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

Interfaces admitidas

- RACADM local

---

clrraclog

Sinopsis

```
racadm clrraclog
```

Descripción

El subcomando **clrraclog** elimina todas las anotaciones existentes del registro del iDRAC. Se crea una nueva anotación para registrar la fecha y la hora en que el registro fue borrado.

---

getsel

En la tabla A-20 se describe el comando **getsel**.

Tabla A-20. getsel

Comando	Definición
getsel -i	Muestra el número de anotaciones en el **Registro de sucesos del sistema**.
getsel	Muestra las anotaciones del registro de sucesos del sistema.

Sinopsis

```
racadm getsel -i

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

Descripción

El comando **getsel -i** muestra el número de anotaciones en registro de sucesos del sistema.

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

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

Tabla A-21. Opciones del subcomando getsel

Opción	Descripción
-A	Especifica que el mensaje de salida debe aparecer sin encabezados ni etiquetas.
-c	Proporciona la cuenta máxima de anotaciones a generar.
-o	Muestra el mensaje de salida en una sola línea.
-s	Especifica la anotación inicial a partir de la cual se muestra la información.
-E	Coloca los 16 bytes del registro de sucesos del sistema sin procesar al final de cada línea de salida como una secuencia de valores hexadecimales.
-R	Sólo se imprimen los datos sin procesar.
-m	Muestra una pantalla de información a la vez y pide al usuario que continúe (es parecida al comando **more** de UNIX).

Salida

El mensaje de salida predeterminado muestra el número de anotación, la fecha y la hora, la severidad y la descripción.

Por ejemplo:

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

Interfaces admitidas

- RACADM local

---

clrsel

Sinopsis

```
racadm clrsel
```

Descripción

El comando **clrsel** elimina todas las anotaciones existentes del **Registro de sucesos del sistema (SEL)**.

Interfaces admitidas

- RACADM local

---

gettracelog

En la tabla A-22 se describe el subcomando **gettracelog**.

Tabla A-22. gettracelog

Comando	Definición
gettracelog -i	Muestra el número de anotaciones en el **registro de rastreo del iDRAC**.
gettracelog	Muestra el **registro de rastreo de iDRAC**.

Sinopsis

```
racadm gettracelog -i

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

Descripción

El comando **gettracelog** (sin la opción **-i**) lee las anotaciones. Las anotaciones de **gettracelog** siguientes se usan para leer anotaciones:

Tabla A-23. Opciones del subcomando gettracelog

Opción	Descripción
-i	Muestra el número de anotaciones en el **registro de rastreo del iDRAC**.
-m	Muestra una pantalla de información a la vez y pide al usuario que continúe (es parecida al comando **more** de UNIX).
-o	Muestra el mensaje de salida en una sola línea.
-c	Especifica el número de anotaciones a mostrar.
-s	Especifica la anotación inicial a mostrar.
-A	No mostrar encabezados ni etiquetas.

Salida

El mensaje de salida predeterminado muestra el número de anotación, la fecha y la hora, el origen y la descripción. La fecha y hora comienza a la media noche del 1º de enero y avanza hasta que el sistema administrado se inicia. Después de que el sistema administrado se inicia, la hora de sistema del mismo se usa para registrar la fecha y hora.

Por ejemplo:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Interfaces admitidas

- RACADM local

---

sslcsrgen

En la tabla A-24 se describe el subcomando **sslcsrgen**.

Tabla A-24. sslcsrgen

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

Sinopsis

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

racadm sslcsrgen -s
```

Descripción

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

Opciones

En la tabla A-25 se describen las opciones del subcomando **sslcsrgen**.

Tabla A-25. Opciones del subcomando sslcsrgen

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

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

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

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

- La CSR se generó de manera satisfactoria.
- La CSR no existe.
- Generación de la CSR en progreso.

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

Ejemplos

```
racadm sslcsrgen -s

o

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

Interfaces admitidas

- RACADM local

---

sslcertupload

En la tabla A-26 se describe el subcomando **sslcertupload**.

Tabla A-26. sslcertupload

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

Sinopsis

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

Opciones

En la tabla A-27 se describen las opciones del subcomando **sslcertupload**.

Tabla A-27. Opciones del subcomando sslcertupload

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

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

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertdownload

En la tabla A-28 se describe el subcomando **sslcertdownload**.

Tabla A-28. sslcertdownload

Subcomando	Descripción
sslcertdownload	Descarga un certificado SSL del RAC al sistema de archivos del cliente.

Sinopsis

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

Opciones

En la tabla A-29 se describen las opciones del subcomando **sslcertdownload**.

Tabla A-29. Opciones del subcomando sslcertdownload

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

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

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertview

En la tabla A-30 se describe el subcomando **sslcertview**.

Tabla A-30. sslcertview

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

Sinopsis

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

Opciones

En la tabla A-31 se describen las opciones del subcomando **sslcertview**.

Tabla A-31. Opciones del subcomando sslcertview

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

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1

Serial Number            : 00
```

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

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

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

```
racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces admitidas

- RACADM local

---

testemail

En la tabla A-32 se describe el subcomando **testemail**.

Tabla A-32. Configuración de testemail

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

Sinopsis

```
racadm testemail -i <indice>
```

Descripción

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

Antes de ejecutar el comando testemail, asegúrese de que el índice especificado en el grupo **cfgEmailAlert** de RACADM esté activado y configurado correctamente. La tabla A-33 proporciona un ejemplo de comandos para el grupo **cfgEmailAlert.**

Tabla A-33. Configuración de testemail

Acción	Comando
Activa la alerta	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Establece la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 usuario1@mi_empresa.com
Establece el mensaje personalizado que se envía a la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "Esta es una prueba"

Comprueba que la dirección IP SNMP esté configurada correctamente	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 192.168.0.152
Muestra la configuración actual de las alertas por correo electrónico	racadm getconfig -g cfgEmailAlert -i *<índice>* donde *<índice>* es un número de 1 a 4

Opciones

En la tabla A-34 se describen las opciones del subcomando **testemail**.

Tabla A-34. Opción del subcomando testemail

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

Salida

Ninguno.

Interfaces admitidas

- RACADM local

---

testtrap

En la tabla A-35 se describe el subcomando **testtrap**.

Tabla A-35. testtrap

Subcomando	Descripción
testtrap	Prueba el componente de alertas de captura SNMP del iDRAC.

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

El subcomando **testtrap** prueba el componente de alertas de capturas SNMP del iDRAC mediante el envío de una captura de prueba del iDRAC a un receptor de capturas de destino especificado en la red.

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

La tabla A-36 muestra una lista y los comandos asociados con el grupo **cfgIpmiPet**.

Tabla A-36. Comandos de alerta de cfg de correo electrónico

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

Entrada

En la tabla A-37 se describen las opciones del subcomando **testtrap**.

Tabla A-37. Opciones del subcomando testtrap

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

Interfaces admitidas

- RACADM local

Regresar a la página de contenido

Regresar a la página de contenido

Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

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

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

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

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

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

idRacProductInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

Integrated Dell Remote Access Controller

Descripción

Una cadena de texto que identifica el producto.

idRacDescriptionInfo (sólo lectura)

Valores legales

Cadena de hasta 255 caracteres ASCII.

Predeterminado

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

Descripción

Una descripción de texto del tipo de RAC.

idRacVersionInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

1.0

Descripción

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

idRacBuildInfo (sólo lectura)

Valores legales

Cadena de hasta 16 caracteres ASCII.

Predeterminado

La versión actual de la compilación de software del RAC. Por ejemplo, "05.12.06".

Descripción

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

idRacName (sólo lectura)

Valores legales

Cadena de hasta 15 caracteres ASCII.

Predeterminado

iDRAC

Descripción

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

idRacType (sólo lectura)

Predeterminado

8

Descripción

Identifica el tipo de controlador de acceso remoto como iDRAC.

---

cfgLanNetworking

Este grupo contiene parámetros para configurar el NIC de iDRAC.

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

cfgDNSDomainNameFromDHCP (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgDNSDomainName (lectura/escritura)

Valores legales

Cadena de hasta 250 caracteres ASCII. Al menos uno de los caracteres debe ser alfabético. Los caracteres permitidos son los alfanuméricos, '-' (guión) y '.' (punto).

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

Predeterminado

""

Descripción

El nombre de dominio DNS. Este parámetro sólo es válido si **cfgDNSDomainNameFromDHCP** se establece como 0 (FALSO).

cfgDNSRacName (lectura/escritura)

Valores legales

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

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

Predeterminado

rac-*etiqueta_de_servicio*

Descripción

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

cfgDNSRegisterRac (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Registra el nombre del iDRAC en el servidor DNS.

cfgDNSServersFromDHCP (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgDNSServer1 (lectura/escritura)

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Descripción

Especifica la dirección IP del servidor DNS 1. Esta propiedad sólo es válida si **cfgDNSServersFromDHCP** se establece como **0** (FALSO).

NOTA: **cfgDNSServer1** y **cfgDNSServer2** se pueden establecer con valores idénticos mientras se intercambian direcciones.

cfgDNSServer2 (lectura/escritura)

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Predeterminado

0.0.0.0

Descripción

Recupera la dirección IP del servidor DNS 2. Este parámetro sólo es válido si **cfgDNSServersFromDHCP** se establece como 0 (FALSO).

NOTA: **cfgDNSServer1** y **cfgDNSServer2** se pueden establecer con valores idénticos mientras se intercambian direcciones.

cfgNicEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el controlador de interfaz de red del iDRAC. Si el NIC está desactivado, las interfaces de red remotas al iDRAC ya no estarán accesibles y sólo se podrá acceder al iDRAC por medio de la interfaz de RACADM local.

cfgNicIpAddress (lectura/escritura)

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

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Predeterminado

192.168.0.*n*

donde *n* es 120 más el número de ranura del servidor.

Descripción

Especifica la dirección IP estática que se asignará al RAC. Esta propiedad sólo es válida si **cfgNicUseDhcp** se establece como **0** (FALSO).

cfgNicNetmask (lectura/escritura)

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

Valores legales

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

Predeterminado

255.255.255.0

Descripción

La máscara de subred que se utiliza para la asignación estática de la dirección IP del iDRAC. Esta propiedad sólo es válida si **cfgNicUseDhcp** se establece como **0** (FALSO).

cfgNicGateway (lectura/escritura)

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

Valores legales

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

Predeterminado

192.168.0.1

Descripción

La dirección IP de puerta de enlace que se utiliza para la asignación estática de la dirección IP del RAC. Esta propiedad sólo es válida si **cfgNicUseDhcp** se establece como **0** (FALSO).

cfgNicUseDhcp (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgNicMacAddress (sólo lectura)

Valores legales

Una cadena que representa la dirección MAC de la tarjeta de interfaz de red del RAC.

Predeterminado

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

Descripción

La dirección MAC del NIC del iDRAC.

---

cfgUserAdmin

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

Se permiten hasta 16 instancias del grupo de usuario. Cada instancia representa la configuración de un usuario individual.

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

Valores legales

2 (**Usuario**)

3 (Operador)

4 (**Administrador**)

15 (**Sin acceso**)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

cfgUserAdminPrivilege (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

0x00000000

Descripción

Esta propiedad especifica los privilegios de autoridad basada en funciones que se otorgan al usuario. El valor se representa como máscara de bits que permite definir cualquier combinación de valores de privilegios. La tabla B-1 describe los valores de bit de privilegio del usuario que se pueden combinar para crear máscaras de bit.

Tabla B-1. Máscaras de bit para privilegios del usuario

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

Ejemplos

La tabla B-2 contiene ejemplos de las máscaras de bits de privilegios para usuarios con uno o más privilegios.

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

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

cfgUserAdminUserName (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 16

Predeterminado

""

Descripción

El nombre del usuario para este índice. El índice de usuario se crea al escribir una cadena en el campo de este nombre si el índice está vacío. Al escribir una cadena de comillas ("") se elimina al usuario de ese índice. No se puede cambiar el nombre. Debe eliminar y luego volver a crear el nombre. La cadena no debe tener / (diagonales), \ (diagonales invertidas), . (puntos), @ (arrobas) ni comillas.

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

cfgUserAdminPassword (de sólo escritura)

Valores legales

Una cadena de hasta 20 caracteres ASCII.

Predeterminado

""

Descripción

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

cfgUserAdminEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva un usuario individual.

cfgUserAdminSolEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el acceso del usuario a la Conexión serie en la LAN (SOL).

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

Este parámetro se debe establecer en función de las instancias existentes.

Descripción

El índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica la dirección de correo electrónico de destino para alertas por correo electrónico. Por ejemplo, usuario1@empresa.com.

cfgEmailAlertAddress

Valores legales

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

Predeterminado

""

Descripción

La dirección de correo electrónico del origen de la alerta.

cfgEmailAlertCustomMsg

Valores legales

Cadena. Cantidad máxima de caracteres = 32.

Predeterminado

""

Descripción

Especifica el mensaje personalizado que se enviará con la alerta.

---

cfgSessionManagement

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

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

cfgSsnMgtConsRedirMaxSessions (lectura/escritura)

Valores legales

De 1 a 2

Predeterminado

2

Descripción

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

cfgSsnMgtWebserverTimeout (lectura/escritura)

Valores legales

De 60 a 1920

Predeterminado

300

Descripción

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

La finalización de una sesión de servidor web cierra la sesión actual.

cfgSsnMgtSshIdleTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

300

Descripción

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

Cuando una sesión Secure Shell ha finalizado, muestra el siguiente mensaje de error sólo después de que usted presione <Entrar>:

```
Advertencia: la sesión ya no es válida, es posible que se haya agotado el tiempo de espera
```

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

cfgSsnMgtTelnetIdleTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

300

Descripción

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

Cuando una sesión Telnet haya finalizado, mostrará el siguiente mensaje de error sólo después de que usted presione <Entrar>:

```
Advertencia: la sesión ya no es válida, es posible que haya agotado el tiempo de espera
```

Después de que el mensaje aparece, el sistema regresa al shell que generó la sesión Telnet.

---

cfgSerial

Este grupo contiene parámetros de configuración de los servicios de iDRAC.

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

cfgSerialSshEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgSerialTelnetEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgRacTuning

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

cfgRacTuneHttpPort (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

80

Descripción

Especifica el número de puerto que se utiliza para la comunicación de red HTTP con el RAC.

cfgRacTuneHttpsPort (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

443

Descripción

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

cfgRacTuneIpRangeEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de validación de rango de dirección IP del iDRAC.

cfgRacTuneIpRangeAddr

Valores legales

Cadena formateada como dirección IP. Por ejemplo: 192.168.0.44.

Predeterminado

192.168.1.1

Descripción

Especifica el patrón de bits de dirección IP aceptable en posiciones determinadas por unos en la propiedad de máscara de rango (**cfgRacTuneIpRangeMask**).

cfgRacTuneIpRangeMask

Valores legales

Valores de máscara de IP estándares con bits justificados a la izquierda

Predeterminado

255.255.255.0

Descripción

Cadena formateada como dirección IP. Por ejemplo: 255.255.255.0.

cfgRacTuneIpBlkEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de bloqueo de direcciones IP del RAC.

cfgRacTuneIpBlkFailCount

Valores legales

De 2 a 16

Predeterminado

5

Descripción

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

cfgRacTuneIpBlkFailWindow

Valores legales

De 10 a 65535

Predeterminado

60

Descripción

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

cfgRacTuneIpBlkPenaltyTime

Valores legales

De 10 a 65535

Predeterminado

300

Descripción

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

cfgRacTuneSshPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

22

Descripción

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

cfgRacTuneTelnetPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

23

Descripción

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

cfgRacTuneConRedirEncryptEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Cifra el vídeo en una sesión de redirección de consola.

cfgRacTuneConRedirPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

5900

Descripción

Especifica el puerto que se debe usar para tráfico de teclado y mouse durante la actividad de redirección de consola con el iDRAC.

cfgRacTuneConRedirVideoPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

5901

Descripción

Especifica el puerto que se debe usar para el tráfico de vídeo durante la actividad de redirección de consola con el iDRAC.

NOTA: Este objeto requiere de un restablecimiento de iDRAC antes de activarse.

cfgRacTuneAsrEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

Activa o desactiva la función de captura de pantallas de último bloqueo del iDRAC.

NOTA: Este objeto requiere de un restablecimiento de iDRAC antes de activarse.

cfgRacTuneWebserverEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgRacTuneLocalServerVideo (lectura/escritura)

Valores legales

1 (activa)

0 (desactiva)

Predeterminado

1

Descripción

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

cfgRacTuneLocalConfigDisable (lectura / escritura)

Valores legales

0 (activa)

1 (desactiva)

Predeterminado

0

Descripción

Desactiva el acceso de escritura a los datos de configuración de iDRAC. La opción predeterminada es el acceso activo.

NOTA: El acceso puede desactivarse utilizando la interfaz local RACADM o la interfaz web; sin embargo, una vez desactivado, el acceso puede reactivarse solamente a través de la interfaz web de iDRAC.

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (lectura / escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

""

Descripción

El nombre de host del servidor administrado.

ifcRacMnOsOsName (lectura / escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

""

Descripción

El nombre del sistema operativo del servidor administrado.

---

cfgRacSecurity

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

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

cfgSecCsrCommonName (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica el nombre común (CN) de la CSR.

cfgSecCsrOrganizationName (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la unidad organizacional (OU) de la CSR.

cfgSecCsrLocalityName (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la localidad (L) de la CSR.

cfgSecCsrStateName (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrCountryCode (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 2.

Predeterminado

""

Descripción

Especifica el código de país (CC) de la CSR

cfgSecCsrEmailAddr (lectura/escritura)

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la dirección de correo electrónico de CSR.

cfgSecCsrKeySize (lectura / escritura)

Valores legales

1024

2048

4096

Predeterminado

1024

Descripción

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

---

cfgRacVirtual

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

cfgVirMediaAttached (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

NOTA: Para activar todos los cambios, deberá reiniciar el sistema.

cfgVirAtapiSrvPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

3668

Descripción

Especifica el número de puerto que se usa para las conexiones cifradas de medios virtuales con el iDRAC.

cfgVirAtapiSrvPortSsl (lectura / escritura)

Valores legales

Cualquier número de puerto que no se esté utilizando, decimal entre 0 y 65535.

Predeterminado

3670

Descripción

Define el puerto que se usa para las conexiones de medios virtuales de SSL.

cfgVirMediaBootOnce (lectura / escritura)

Valores legales

1 (activado)

0 (desactivado)

Predeterminado

0

Descripción

Activa o desactiva la función de iniciar una vez a partir de los medios virtuales del iDRAC. Si esta propiedad está activada al momento de reiniciar el servidor host, la función intentará iniciar a partir de los dispositivos de medios virtuales; si hay medios adecuados instalados en el dispositivo.

cfgFloppyEmulation (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgActiveDirectory

Este grupo contiene parámetros para configurar la característica Active Directory de iDRAC.

cfgADRacDomain (lectura / escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número de caracteres está limitado a 254.

Predeterminado

""

Descripción

El dominio de Active Directory donde reside el DRAC.

cfgADRacName (lectura / escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número de caracteres está limitado a 254.

Predeterminado

""

Descripción

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

cfgADEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la autentificación de usuario de Active Directory en el iDRAC. Si esta propiedad está desactivada, se utilizará la autentificación local de iDRAC para los inicios de sesión de usuarios.

cfgADAuthTimeout (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el iDRAC**.

Valores legales

De 15 a 300

Predeterminado

120

Descripción

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

cfgADRootDomain (lectura / escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número de caracteres se limita a 254.

Predeterminado

""

Descripción

Dominio raíz del bosque de dominios.

cfgADSpecifyServerEnable (lectura / escritura)

Valores legales

1 ó 0 (verdadero o falso).

Predeterminado

0

Descripción

1 (verdadero) permite especificar un LDAP o un servidor de catálogo global. 0 (falso) desactiva esta opción.

cfgADDomainController (lectura / escritura)

Dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

Ningún valor predeterminado

Descripción

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

cfgADGlobalCatalog (lectura/escritura)

Valores legales

Dirección IP válida o un nombre de dominio completo (FQDN)

Predeterminado

Ningún valor predeterminado

Descripción

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

cfgADType (lectura/escritura)

Valores legales

1 = activa Active Directory con el esquema ampliado.

2 = activa Active Directory con el esquema estándar.

Predeterminado

1 = esquema ampliado

Descripción

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

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

Número entero de 1 a 5.

Descripción

Índice del grupo de funciones según está registrado en Active Directory.

cfgSSADRoleGroupName (lectura/escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número de caracteres está limitado a 254.

Predeterminado

(vacío)

Descripción

Índice del grupo de funciones según está registrado en bosque de Active Directory.

cfgSSADRoleGroupDomain (lectura/escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número de caracteres está limitado a 254.

Predeterminado

(vacío)

Descripción

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

cfgSSADRoleGroupPrivilege (lectura/escritura)

Valores legales

De **0x00000000** a **0x000001ff**

Predeterminado

(vacío)

Descripción

Utilice los números de máscara de bits que aparecen en la tabla B-3 para establecer los privilegios de autoridad en base a función para un grupo de funciones.

Tabla B-3. Máscaras de bits para los Privilegios del grupo de funciones

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

cfgIpmiSol

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

cfgIpmiSolEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva SOL.

cfgIpmiSolBaudRate (lectura/escritura)

Valores legales

19200, 57600, 115200

Predeterminado

115200

Descripción

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

cfgIpmiSolMinPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSolAccumulateInterval (lectura/escritura)

Valores legales

De 1 a 255.

Predeterminado

10

Descripción

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

cfgIpmiSolSendThreshold (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

255

Descripción

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

---

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de IPMI en la LAN.

cfgIpmiLanPrivLimit (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiLanAlertEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

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

cfgIpmiEncryptionKey (lectura/escritura)

Valores legales

Una cadena de dígitos hexadecimales de 0 a 20 caracteres sin espacios.

Predeterminado

00000000000000000000

Descripción

La clave de cifrado de IPMI.

cfgIpmiPetCommunityName (lectura/escritura)

Valores legales

Una cadena de hasta 18 caracteres.

Predeterminado

público

Descripción

El nombre de comunidad SNMP para las capturas.

---

cfgIpmiPef

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

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

cfgIpmiPefName (sólo lectura)

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

El nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de sucesos de plataforma.

cfgIpmiPefIndex (sólo lectura)

Valores legales

De 1 a 17

Predeterminado

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

Descripción

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

cfgIpmiPefAction (lectura/escritura)

Valores legales

0 (ninguno)

1 (apagar)

2 (restablecer)

3 (ciclo de encendido)

Predeterminado

0

Descripción

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

cfgIpmiPefEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva un filtro de sucesos de plataforma específico.

---

cfgIpmiPet

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

cfgIpmiPetIndex (lectura/escritura)

Valores legales

De 1 a 4

Predeterminado

El valor de índice correspondiente.

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

Valores legales

Cadena que representa una dirección IP válida. Por ejemplo: `192.168.0.67`.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP de destino del receptor de capturas en la red. El receptor de capturas recibe una captura SNMP cuando se presenta un suceso en el servidor administrado.

cfgIpmiPetAlertEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva una captura específica.

Regresar a la página de contenido

Regresar a la página de contenido

Base de datos de propiedades iDRAC SMCLP

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

/system1/sp1/account<1-16>

Este grupo ofrece información de configuración de los usuarios locales que tienen acceso al RAC por medio de las interfaces remotas disponibles. Se permiten hasta 16 casos del grupo de usuario. Cada caso <1-16> representa la configuración para un usuario local individual.

userid (sólo lectura)

Valores legales

1-16

Predeterminado

Depende de la instancia de cuenta a la que se está accediendo.

Descripción

Especifica la Id. de instancia o la Id. de usuario local.

username (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 16

Predeterminado

""

Descripción

Una cadena de texto que contiene el nombre del usuario local para esta cuenta. La cadena no puede contener diagonal (/), punto (.), arroba (@) ni comillas ("). Para eliminar el usuario, se debe eliminar la cuenta. (eliminar cuenta<1-16>).

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

oemdell_ipmilanprivileges (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

password (sólo escritura)

Valores legales

Una cadena de texto de entre 4 y 20 caracteres de longitud.

Predeterminado

""

Descripción

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

enabledstate (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Ayuda a activar o desactivar a un usuario individual.

soleenables (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva el acceso del usuario a la Conexión serie en la LAN (SOL).

oemdell_extendedprivileges (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

0x00000000

Descripción

Especifica los privilegios de autoridad basada en funciones que se otorgan al usuario. El valor se representa como máscara de bits que permite definir cualquier combinación de valores de privilegios. La tabla C-1 describe los valores de bit de privilegio del usuario que se pueden combinar para crear máscaras de bit.

Tabla C-1. Máscaras de bit para privilegios del usuario

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

Ejemplos

La tabla C-2 contiene ejemplos de las máscaras de bits de privilegios para usuarios con uno o más privilegios.

Tabla C-2. Máscaras de bits para privilegios del usuario

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

/system1/sp1/enetport1/*

Este grupo contiene parámetros para configurar el NIC de iDRAC. Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca el NIC de iDRAC, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP del NIC de iDRAC cerrarán todas las sesiones de usuario activas y requerirán que los usuarios se vuelvan a conectar con la configuración actualizada de la dirección IP.

macaddress (sólo lectura)

Valores legales

Una cadena que representa la dirección MAC de la tarjeta de interfaz de red del RAC.

Predeterminado

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

Descripción

Contiene la dirección MAC del NIC del iDRAC.

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva el controlador de interfaz de red del iDRAC. Si el NIC está desactivado, las interfaces de red remotas al iDRAC se tornan inaccesibles, haciendo que el iDRAC esté disponible solamente mediante interfaz RACADM local.

ipaddress (lectura/escritura)

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Predeterminado

192.168.0.n (en donde n es 120 más el número de ranura del servidor)

Descripción

Especifica la dirección IP estática que se asignará al RAC. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

subnetmask (lectura/escritura)

Valores legales

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

Predeterminado

255.255.255.0

Descripción

La máscara de subred que se usa para la asignación estática de la dirección IP del iDRAC. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

oemdell_usedhcp (lectura / escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Especifica si se usa DHCP para asignar la dirección IP del iDRAC. Si esta propiedad se configura en 1 (activado), entonces la dirección IP del iDRAC, la máscara de subred y la puerta de enlace se asignan a partir del servidor DHCP en la red. Si esta propiedad se configura en 0 (desactivado), la dirección IP estática, la máscara de subred y la puerta de enlace obtienen valores insertados manualmente por el usuario.

asignado (lectura / escritura)

Valores legales

0 (asignación pendiente)

1 (asignado)

Predeterminado

1

Descripción

Permite al usuario cambiar la dirección IP y/o la máscara de subgrupo sin finalizar la sesión actual. Si esta propiedad está configurada en 1 (asignado), la dirección IP y la máscara de subred son válidas. Un cambio en la dirección IP o la máscara de subred convertirá automáticamente esta propiedad a 0 (asignación pendiente). Para que la configuración de red sea válida, la propiedad debe volver a configurarse en 1.

/system1 / sp1 / enetport1 / lanendpt1 / ipendpt1 / dnse ndpt1

oemdell_domainnamefromdhcp (lectura / escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

oemdell_dnsdomainname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII. Al menos uno de los caracteres debe ser alfabético.

Predeterminado

""

Descripción

Contiene el nombre de dominio DNS. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

oemdell_dnsregisterrac (lectura/escritura)

Valores legales

0 (no registrado)

1 (registrado)

Predeterminado

0

Descripción

Registra el nombre del iDRAC en el servidor DNS.

oemdell_dnsracname (lectura/escritura)

Valores legales

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

NOTA: Algunos servidores DNS sólo registran nombres hasta un máximo de 31 caracteres.

Predeterminado

rac-etiqueta_de_servicio

Descripción

Muestra el nombre de RAC, que es la etiqueta de servicio RAC predeterminada. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 1 (desactivado).

oemdell_serversfromdhcp (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap1

dnsserveraddress (lectura/escritura)

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP del servidor DNS 1. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

/system1/sp1/enetport1/lanendpt1/ipendpt1/dnse ndpt1/remotesap2

dnsserveraddress (lectura/escritura)

Valores legales

Una cadena que representa una dirección IP válida. Por ejemplo: 192.168.0.20.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP del servidor DNS 2. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

/system1/sp1/enetport1/lanendpt1/ipendpt1/remot esap1

defaultgatewayaddress (lectura/escritura)

Valores legales

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

Predeterminado

192.168.0.1

Descripción

La dirección IP de puerta de enlace que se usa para la asignación estática de la dirección IP del RAC. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

/system1/sp1/group<1-5>

Estos grupos contienen parámetros para ajustar la configuración del esquema estándar de Active Directory.

oemdell_groupname (lectura/escritura)

Valores legales

Cualquier cadena de texto que pueda imprimirse con un máximo de 254 caracteres sin espacios en blanco.

Predeterminado

""

Descripción

Contiene el nombre del grupo de funciones según está registrado en bosque de Active Directory.

oemdell_groupdomain (lectura/escritura)

Valores legales

Cualquier cadena de texto que pueda imprimirse con un máximo de 254 caracteres sin espacios en blanco.

Predeterminado

""

Descripción

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

oemdell_groupprivilege (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

""

Descripción

Use los números de máscara de bits de la Tabla B-3 para establecer los privilegios de autoridad en base a función para un grupo de funciones.

Tabla C-3. Máscaras de bits para los Privilegios del grupo de funciones

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

/system1/sp1/oemdell_adservice1

Este grupo contiene parámetros para configurar la característica Active Directory de iDRAC.

enabledstate (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

oemdell_adracname (lectura/escritura)

Valores legales

Cualquier cadena de texto que pueda imprimirse con un máximo de 254 caracteres sin espacios en blanco.

Predeterminado

""

Descripción

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

oemdell_adracdomain (lectura/escritura)

Valores legales

Cualquier cadena de texto que pueda imprimirse con un máximo de 254 caracteres sin espacios en blanco.

Predeterminado

""

Descripción

El dominio de Active Directory en donde reside el iDRAC.

oemdell_adrootdomain (lectura/escritura)

Valores legales

Cualquier cadena de texto que pueda imprimirse con un máximo de 254 caracteres sin espacios en blanco.

Predeterminado

""

Descripción

Dominio raíz del bosque de dominios.

oemdell_timeout (lectura/escritura)

Valores legales

De 15 a 300

Predeterminado

120

Descripción

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

oemdell_schematype (lectura/escritura)

Valores legales

1 (esquema extendido)

2 (esquema estándar)

Predeterminado

1

Descripción

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

oemdell_adspecifyserverenable (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Permite al usuario especificar un servidor LDAP o Catálogo global.

oemdell_addomaincontroller (lectura/escritura)

Valores legales

Una dirección IP válida o un nombre de dominio calificado (FQDN).

Predeterminado

""

Descripción

Valor especificado por el usuario que el iDRAC usa para buscar nombres de usuarios en el servidor LDAP.

oemdell_adglobalcatalog (lectura/escritura)

Valores legales

Una dirección IP válida para un FQDN.

Predeterminado

Ningún valor predeterminado

Descripción

Valor especificado por el usuario que el iDRAC usa para buscar nombres de usuarios en el servidor LDAP.

/system1/sp1/oemdell_racsecurity1

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

commonname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

organizationname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_organizationunit (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_localityname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica la localidad de la CSR.

oemdell_statename (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_countrycode (lectura/escritura)

Valores legales

Una cadena de hasta 2 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el código de país de la CSR.

oemdell_emailaddress (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica la dirección de correo electrónico de CSR.

oemdell_keysize (lectura/escritura)

Valores legales

1024

2048

4096

Predeterminado

1024

Descripción

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

/system1/sp1/oemdell_ssl1

Contiene los parámetros necesarios para generar solicitudes de firma de certificado (CSR) y ver los certificados.

generate (lectura/escritura)

Valores legales

0 (no generar)

1 (generar)

Predeterminado

0

Descripción

Si está configurado en 1, genera una CSR. Deben configurarse primero las propiedades en el destino oemdell_racsecurity1 antes de generar una CSR.

oemdell_status (sólo lectura)

Valores legales

No se encuentra CSR

CSR generada

Predeterminado

No se encuentra CSR

Descripción

Muestra el estado del comando generar emitido anteriormente, de existir, durante la sesión actual.

oemdell_certtype (lectura/escritura)

Valores legales

SSL

AD

CSR

Predeterminado

SSL

Descripción

Especifica el tipo de certificado que se verá (AD o SSL) y permite generar una CRS con la ayuda de la propiedad **generar**.

/system1/sp1/oemdell_vmservice1

Este grupo contiene parámetros para configurar la función de medios virtuales de iDRAC.

enabledstate (lectura/escritura)

Valores legales

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

Predeterminado

VMEDIA_ATTACH

Descripción

Se usa para conectar dispositivos virtuales al sistema mediante el bus USB, permitiendo al servidor reconocer dispositivos de almacenamiento masivo USB conectados al sistema. Esto equivale a conectar un CD-ROM USB local, o unidad de disquete, a un puerto USB del sistema. Cuando los dispositivos estén conectados, usted podrá conectar los dispositivos virtuales de manera remota usando la interfaz web de iDRAC o la CLI. Si asigna el valor de 0 a esta propiedad, hará que los dispositivos se desconecten del bus USB.

oemdell_singleboot (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva la función de iniciar una vez a partir de los medios virtuales del iDRAC. Si esta propiedad está desactivada cuando se reinicia el servidor host, el servidor intentará reiniciarse de todos los dispositivos multimedia virtuales.

oemdell_floppyemulation (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

/system1/sp1/oemdell_vmservice1/tcpendpt1

portnumber (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

3668

Descripción

Especifica el número de puerto que se usa para las conexiones cifradas de medios virtuales con el iDRAC.

oemdell_sslenabled (sólo lectura)

Valor legal

FALSE

Predeterminado

FALSE

Descripción

Indica que el puerto tiene SSL desactivado.

portnumber (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

3670

Descripción

Especifica el número de puerto que se usa para las conexiones cifradas de medios virtuales con el iDRAC.

oemdell_sslenabled (sólo lectura)

Valor legal

TRUE

Predeterminado

TRUE

Descripción

Indica que el puerto tiene SSL desactivado.

Regresar a la página de contenido

Regresar a la página de contenido

Equivalencias de RACADM y SM-CLP

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

La tabla D-1 muestra una lista de los grupos y objetos de RACADM y, cuando así corresponde, los lugares equivalentes de SM-SLP en el MAP de SM-CLP.

Tabla D-1. Grupos y objetos de RACADM y equivalencias de SM-CLP

Grupos y objetos de RACADM	SM-CLP	Descripción
idRacInfo		
idRacName		Cadena de hasta 15 caracteres ASCII. Valor predeterminado: **iDRAC**.
idRacProductInfo		Cadena de hasta 63 caracteres ASCII. Valor predeterminado: **Integrated Dell Remote Access Controller**.
idRacDescriptionInfo		Cadena de hasta 255 caracteres ASCII Valor predeterminado: **Este componente de sistema proporciona un conjunto completo de funciones de administración remota para los servidores Dell PowerEdge**
idRacVersionInfo		Cadena de hasta 63 caracteres ASCII. Valor predeterminado: **1**
idRacBuildInfo		Cadena de hasta 16 caracteres ASCII.
idRacType		Valor predeterminado: **8**
cfgActiveDirectory	**/system1/sp1/oemdell_adservice1**	
cfgADEnable	enablestate	0 para desactivar, 1 para activar. Valor predeterminado: **0**
cfgADRacName	oemdell_adracname	Una cadena de hasta 254 caracteres.
cfgADRacDomain	oemdell_adracdomain	Una cadena de hasta 254 caracteres.
cfgADRootDomain	oemdell_adrootdomain	Una cadena de hasta 254 caracteres.
cfgADAuthTimeout	oemdell_timeout	De 15 a 300 segundos. Valor predeterminado: **120**
cfgADType	oemdell_schematype	1 para esquema estándar, 2 para esquema ampliado. Valor predeterminado: **1**
cfgADSpecifyServerEnable	oemdell_adspecifyserverenable	Cuando se activa, especifica un LDAP o un servidor de catálogo global. 0 para desactivar, 1 para activar. Valor predeterminado: **0**
cfgADDomainController	oemdell_addomaincontroller	El nombre DNS o la dirección IP del controlador de dominio que se usa en la búsqueda de LDAP.
cfgADGlobalCatalog	oemdell_adglobalcatalog	El nombre DNS o la dirección IP del controlador de dominio que se usa en la búsqueda de LDAP.
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1** a **/system1/sp1/group5**	RACADM: identificación de índice de grupo (1-5). SM-CLP: se selecciona con la ruta de acceso de la dirección.
cfgSSADRoleGroupName	oemdell_groupname	Una cadena de hasta 254 caracteres.
cfgSSADRoleGroupDomain	oemdell_groupdomain	Una cadena de hasta 254 caracteres.
cfgSSADRoleGroupPrivilege	oemdell_groupprivilege	Máscara de bits con valores entre 0x00000000 y 0x000001ff.
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	La dirección MAC de la interfaz. No se puede editar.
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	0 para desactivar el NIC, 1 para activar el NIC. Valor predeterminado: **0**
cfgNicUseDHCP	oemdell_usedhcp	0 para configurar direcciones de red estáticas, 1 para usar DHCP. Valor predeterminado: **0**
cfgNicIpAddress	ipaddress	La dirección IP del iDRAC. Valor predeterminado: **192.168.0.120** más el número de ranura del servidor.
cfgNicNetmask	subnetmask	La máscara de subred para la red de iDRAC. Valor

		predeterminado: **255.255.255.0**
	comprometidos	Cuando los valores del grupo cambian, **comprometidos** tiene el valor 0 para indicar que los nuevos valores no han sido guardados. Establezca el valor en 1 para guardar la nueva configuración. Valor predeterminado: **1**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	Cadena de hasta 250 caracteres ASCII. Al menos un carácter debe ser alfabético.
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	Establezca el valor 1 para obtener el nombre de dominio de DHCP. Valor predeterminado: **0**
cfgDNSRacName	oemdell_dnsracname	Cadena de hasta 63 caracteres ASCII. Al menos un carácter debe ser alfabético. Valor predeterminado: **iDRAC-***más la etiqueta de servicio de Dell*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	Establezca el valor en 1 para registrar el nombre del iDRAC en el DNS. Valor predeterminado: **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	Establezca el valor en 1 para obtener del DHCP las direcciones de servidor DNS. Valor predeterminado: **0**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Una cadena que represente la dirección IP de un servidor DNS.
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	Una cadena que represente la dirección IP de un servidor DNS.
	/system1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	Una cadena que represente la dirección IP de la puerta de enlace predeterminada. Valor predeterminado: **192.168.0.1**
cfgRacVirtual	**/system1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	Establezca el valor en 1 para activar la emulación de disco flexible. Valor predeterminado: **0**
cfgVirMediaAttached	enabledstate	Establézcala en 1 (RACADM)/ VMEDIA_ATTACH (SM-CLP) para conectar los medios. Valor predeterminado: 1 (RACADM)/ VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdell_singleboot	Establezca el valor en 1 para ejecutar el siguiente inicio a partir de los medios seleccionados. Valor predeterminado **0**.
	/system1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	Establezca el valor en 1 si SSL está activado para el primer dispositivo de medios virtuales y en 0 si no es así. No se puede editar.
cfgVirAtapiSvrPort	portnumber	Puerto para uso del primer dispositivo de medios virtuales. Valor predeterminado: **3668**
	/system1/sp1/oemdell_vmservice1/tcpendpt2	
	oemdell_sslenabled	Establezca el valor en 1 si SSL está activado para el segundo dispositivo de medios virtuales y en 0 si no es así. No se puede editar.
cfgVirAtapiSvrPortSsl	portnumber	Puerto para uso del segundo dispositivo de medios virtuales. Valor predeterminado: **3670**
cfgUserAdmin	**/system1/sp1/account1** ***a*** **/system1/sp1/account16**	
cfgUserAdminEnable	enabledstate	Establezca el valor en 1 para activar el usuario. Valor predeterminado: **0**
cfgUserAdminIndex	userid	Índice de usuario, de 1 a 16.
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2 (usuario), 3 (operador), 4 (administrador) o 15 (Sin acceso). Valor predeterminado: **4**
cfgUserAdminPassword	contraseña	Una cadena de hasta 20 caracteres ASCII.

cfgUserAdminPrivilege	oemdell_extendedprivileges	El valor de la máscara de bits entre 0x00000000 y 0x000001ff. Valor predeterminado: **0x00000000**
cfgUserAdminSolEnable	solenabled	Establezca el valor en 1 para permitir que el usuario use comunicación en serie en la LAN. Valor predeterminado: **0**
cfgUserAdminUserName	nombre de usuario	Cadena de hasta 16 caracteres.
cfgEmailAlert		
cfgEmailAlertAddress		Dirección de destino de correo electrónico, de hasta 64 caracteres.
cfgEmailAlertCustomMsg		Mensaje para enviar en correo electrónico, hasta 32 caracteres.
cfgEmailAlertEnable		Establezca el valor en 1 para activar la alerta por correo electrónico. Valor predeterminado: **0**
cfgEmailAlertIndex		Índice de una instancia de alerta por correo electrónico. Número de 1 a 4.
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Número de sesiones permitidas de redirección de consola simultáneas (1 ó 2). Valor predeterminado: **2**
cfgSsnMgtSshIdleTimeout		Número de segundos de inactividad antes que la sesión SSH agote el tiempo de espera. 0 para desactivar el tiempo de espera o para establecerlo entre 60 y 1920 segundos. Valor predeterminado: **300**
cfgSsnMgtTelnetIdleTimeout		Número de segundos de inactividad antes de que la sesión de Telnet agote el tiempo de espera. 0 para desactivar el tiempo de espera o para establecerlo entre 60 y 1920 segundos. Valor predeterminado: **300**
cfgSsnMgtWebserverTimeout		Número de segundos de inactividad antes de que la sesión de interfaz web agote el tiempo de espera. De 60 a 1920 segundos. Valor predeterminado: **300**
cfgRacTuning		
cfgRacTuneConRedirEnable		Establezca el valor en 1 para activar la redirección de consola o en 0 para desactivarla. Valor predeterminado: **1**
cfgRacTuneConRedirEncrypt Activar		Establezca el valor en 1 para activar el cifrado del tráfico de red de la redirección de consola o en 0 para desactivarlo. Valor predeterminado: **1**
cfgRacTuneConRedirPort		El puerto que se va a usar la redirección de consola. Valor predeterminado: **5900**
cfgRacTuneConRedirVideoPort		El puerto que se va a usar la redirección de vídeo de consola. Valor predeterminado: **5901**
cfgRacTuneHttpPort		Puerto que se va a usar para la interfaz web de HTTP. Valor predeterminado: **80**
cfgRacTuneHttpsPort		Puerto que se va a usar para la interfaz web de HTTPS seguro. Valor predeterminado: **443**
cfgRacTuneIpBlkEnable		Establezca el valor en 1 para activar el bloqueo de IP. Valor predeterminado: **0**
cfgRacTuneIPBlkFailCount		El número de intentos fallidos de inicio de sesión permitidos antes de bloquear la IP (de 2 a 16). Valor predeterminado: **5**
cfgRacTuneIpBlkFailWindow		Periodo en segundos durante el cual se cuentan los intentos fallidos de inicio de sesión (de 10 a 65535). Valor predeterminado: **60**
cfgRacTuneIpBlkPenaltyTime		El periodo en segundos que una IP permanecerá bloqueada (de 10 a 65535). Valor predeterminado: **300**
cfgRacTuneIpRangeAddr		La dirección base para el filtro de rango de IP. Valor predeterminado: **192.168.0.1**
cfgRacTuneIpRangeEnable		Establezca el valor en 1 para activar la filtración de rango de IP. Valor predeterminado: 0
cfgRacTuneIpRangeMask		Máscara de bits que se aplica a la dirección base para seleccionar direcciones IP válidas. Valor predeterminado: **255.255.255.0**
cfgRacTuneLocalServerVideo		Establezca el valor en 1 para activar la consola iKVM local. Valor predeterminado: **1**
cfgRacTuneSshPort		Puerto que se va a usar para el servicio SSH. Valor predeterminado: **22**
cfgRacTuneTelnetPort		Puerto que se va a usar para el servicio Telnet. Valor predeterminado: **23**
cfgRacTuneWebserverEnable		Establezca el valor en 1 para activar la interfaz web de iDRAC. Valor predeterminado: **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		El nombre de host del servidor administrado. Una cadena

		de hasta 255 caracteres.
ifcRacMnOsOsName		Nombre del sistema operativo del servidor administrado. Una cadena de hasta 255 caracteres.
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Nombre común de Active Directory. Una cadena de hasta 254 caracteres.
cfgRacSecCsrCountryCode	oemdell_countrycode	Código de país de Active Directory. 2 caracteres.
cfgRacSecCsrEmailAddr	oemdell_emailaddress	Dirección de correo electrónico que se usa para la solicitud de firma de certificado. Una cadena de hasta 254 caracteres.
cfgRacSecCsrKeySize	oemdell_keysize	Longitud de la clave de cifrado (512, 1024 ó 2048). Valor predeterminado: **1024**.
cfgRacSecCsrLocalityName	oemdell_localityname	Nombre de la localidad de Active Directory. Una cadena de hasta 254 caracteres.
cfgRacSecCsrOrganizationName	organizationname	Nombre de organización de Active Directory. Una cadena de hasta 254 caracteres.
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Nombre de la unidad de organización de Active Directory. Una cadena de hasta 254 caracteres.
cfgRacSecCsrStateName	oemdell_statename	Nombre del estado de Active Directory. Una cadena de hasta 254 caracteres.
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Número máximo de milisegundos a esperar antes de enviar a un paquete de comunicación en serie en la LAN (de 1 a 255). Valor predeterminado: **10**
cfgIpmiSolBaudRate		Velocidad en baudios para uso en la comunicación en serie en la LAN (19200, 57600, 115200). Valor predeterminado: **115200**
cfgIpmiSolEnable		Establezca el valor en 1 para activar la función se comunicación en serie en la LAN. Valor predeterminado: **0**
cfgIpmiSolSendThreshold		Número máximo de caracteres a recopilar antes de enviar datos de SOL (de 1 a 255). Valor predeterminado: **255**
cfgIpmiSolMinPrivilege		Privilegio mínimo requerido para usar la comunicación en serie en la LAN. 2 (usuario), 3 (operador) o 4 (administrador). Valor predeterminado: **4**
cfgIpmiLan		
cfgIpmiEncryptionKey		Una cadena de 0 a 40 dígitos hexadecimales. Valor predeterminado: **00000000000000000000000000000000000000000000**
cfgIpmiLanAlertEnable		Establezca el valor en 1 para activar las alertas de LAN IPMI. Valor predeterminado: **0**
cfgIpmiLanEnable		Establezca el valor en 1 para activar IPMI en la interfaz de LAN. Valor predeterminado: **0**
cfgIpmiPetCommunityName		Una cadena de hasta 18 caracteres. Valor predeterminado: **public**
cfgIpmiPef		
cfgIpmiPefAction		La acción a realizar al detectar el suceso. 0 (ninguna), 1 (apagar), 2 (restablecer), 3 (ciclo de encendido). Valor predeterminado: **0**
cfgIpmiPefEnable		Establezca el valor en 1 para activar el filtro de sucesos de plataforma. Valor predeterminado: **0**
cfgIpmiPefIndex		El número índice del filtro de sucesos de plataforma. (de 1 a 17)
cfgIpmiPefName		El nombre del suceso de plataforma, una cadena de hasta 254 caracteres. No se puede editar.
cfgIpmiPet		
cfgIpmiPetAlertDestIpAddr		La dirección IP del receptor de captura de sucesos de plataforma. Valor predeterminado: **0.0.0.0**
cfgIpmiPetAlertEnable		Establezca el valor en 1 para activar la captura de sucesos de plataforma. Valor predeterminado: **1**
cfgIpmiPetIndex		Número índice (de 1 a 4) de la captura de sucesos de plataforma.

Tabla D-2. Subcomandos de RACADM y equivalencias de SM-CLP

Subcomando de RACADM	SM-CLP	Descripción
sslcsrgen -g	set /system1/sp1/oemdell_ssl1 oemdell_certtype=CSR set /system1/sp1/oemdell_ssl1 generate=1 dump -destination <URI_de_TFTP_de_solicitud_de_firma_de_certificado_del_iDRAC> /system1/sp1/oemdell_ssl1	Genera y descarga una solicitud de firma de certificado (CSR) SSL.
sslcsrgen -s	show /system1/sp1/oemdell_ssl1 oemdell_status	Muestra el estado de un proceso de generación de CSR.
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI_de_TFTP_de_certificado_de_servidor_del_iDRAC> /system1/sp1/oemdell_ssl1	Carga el certificado de servidor del iDRAC en este último.
sslcertupload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1	Carga el certificado de Active Directory en el iDRAC.
sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI_de_TFTP_de_certificado_de_servidor_del_iDRAC> /system1/sp1/oemdell_ssl1	Descarga del iDRAC el certificado de servidor del mismo.
sslcertdownload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1	Descarga del iDRAC el certificado de Active Directory.

Regresar a la página de contenido

Regresar a la página de contenido

Descripción del iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

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

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

Usted puede configurar el iDRAC 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, iDRAC puede registrar datos de suceso y capturar una imagen de la pantalla cuando detecte que el sistema se ha bloqueado.

Los servidores administrados están instalados en un gabinete (chasis) de sistema Dell M1000e con suministros de energía modulares, ventiladores y un controlador de administración de chasis (CMC). El CMC supervisa y administra todos los componentes instalados en el chasis. Se puede agregar un CMC redundante para estar protegido contra fallas en caso de que el CMC principal falle. El chasis ofrece acceso a los iDRAC por medio de la pantalla LCD, las conexiones de consola locales y la interfaz web.

Todas las conexiones de red al iDRAC son a través de la interfaz de red del CMC (el puerto de conexión RJ45 del CMC etiquetado "GB1"). El CMC enruta el tráfico hacia los iDRAC en los servidores por medio de una red privada interna. Esta red de administración privada está fuera de la ruta de acceso de los datos del servidor y fuera del control del sistema operativo, es decir *fuera de banda*. Se puede acceder a las interfaces de red *dentro de banda* de los servidores administrados mediante los módulos de E/S (IOM) instalados en el chasis.

De manera predeterminada, la interfaz de red del iDRAC está desactivada. Se debe configurar antes de que se pueda acceder al iDRAC. Una vez que el iDRAC esté activado y configurado en la red, se podrá tener acceso a la dirección IP asignada del mismo por medio de la interfaz web del iDRAC, Telnet o SSH y los protocolos de administración de red admitidos, por ejemplo, la Interfaz de administración de plataforma inteligente (IPMI).

Funciones administrativas de iDRAC

El iDRAC ofrece las siguientes funciones administrativas:

- Registro de Sistema dinámico de nombres de dominio (DDNS)
- Administración y supervisión de sistemas remotos por medio de una interfaz web, la interfaz de línea de comandos RACADM local a través de la redirección de consola y la línea de comandos SM-CLP mediante una conexión Telnet/SSH
- Compatibilidad con la autenticación de Microsoft Active Directory®: centraliza las identificaciones y contraseñas de usuario de iDRAC en Active Directory por medio del esquema estándar o de un esquema ampliado
- Redirección de consola: brinda las funciones de teclado, vídeo y mouse de sistema remoto
- Medios virtuales: activa un servidor administrado para tener acceso a una unidad local de medios en la estación de administración o a imágenes ISO de CD/DVD en un recurso compartido de red
- Supervisión: brinda acceso a la información del sistema y al estado de los componentes
- Acceso a los registros del sistema: brinda acceso al registro de sucesos de sistema, el registro del iDRAC y la pantalla último bloqueo del sistema bloqueado o que no responde y es independiente del estado del sistema operativo
- Integración del software Dell OpenManage: permite activar la interfaz web del iDRAC a partir de Dell OpenManage Server Administrator o IT Assistant
- Alerta de iDRAC: envía alertas sobre problemas potenciales de los nodos administrados por medio de mensajes de correo electrónico o capturas SNMP
- Administración remota de la alimentación: brinda funciones de administración remota de la alimentación, como el apagado y restablecimiento, a partir de una consola de administración
- Compatibilidad con la Interfaz de administración de plataforma inteligente (IPMI)
- Cifrado de Capa de conexión segura (SSL): ofrece administración remota y segura de sistemas por medio de la interfaz web
- Administración de seguridad de nivel de contraseña: evita el acceso no autorizado a un sistema remoto
- Autoridad en base a funciones: proporciona permisos asignables para distintas tareas de administración de sistemas

---

Características de seguridad del iDRAC

El iDRAC tiene las siguientes características de seguridad:

- Autenticación de usuarios por medio de Microsoft Active Directory (opcional) o identificaciones y contraseñas de usuarios guardadas en hardware

- Autoridad en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de identificación y contraseña de usuario por medio de la interfaz web o SM-CLP
- Las interfaces SM-CLP y web interfaces, que son compatibles con los cifrados de 128 bit y 40 bit (para países en los que no se aceptan 128 bits), usando el estándar SSL 3.0
- Configuración del tiempo de espera de la sesión (en segundos) por medio de la interfaz web o SM-CLP
- Puertos IP que se pueden configurar (en los casos correspondientes)

  NOTA: Telnet no admite el cifrado SSL.

- Secure Shell (SSH), que usa una capa de transporte cifrado para ofrecer mayor seguridad
- Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando ésta ha superado el límite
- Rango limitado de direcciones IP para clientes que se conectan al iDRAC

Plataformas Admitidas

El iDRAC admite los siguientes sistemas PowerEdge en el gabinete de sistema Dell PowerEdge M1000e:

- PowerEdge M600
- PowerEdge M605
- PowerEdge M805
- PowerEdge M905

Lea el archivo léame del iDRAC y la *Guía de compatibilidad de Dell PowerEdge* que se encuentra en el sitio web de asistencia Dell Support en **support.dell.com** para conocer las plataformas compatibles más recientes.

Sistemas operativos admitidos

La tabla 1-1 muestra una lista de los sistemas operativos que el iDRAC admite.

Consulte la *Guía de compatibilidad de Dell OpenManage Server Administrator* que se encuentra en el sitio web de asistencia Dell Support en **support.dell.com** para obtener la información más reciente.

Tabla 1-1. Sistemas operativos admitidos

Familia de sistemas operativos	Sistema operativo
Microsoft Windows	Microsoft® Windows Server® 2003 R2 ediciones Standard y Enterprise (x86 de 32 bits) con SP2 Microsoft Windows Server 2003 ediciones Standard y Enterprise (x86 de 32 bits) con SP2 Microsoft Windows Server 2003 Standard Edition y Enterprise (x64) Edition con SP2 Microsoft Windows Storage Server 2003 R2, ediciones Express, Workgroup, Standard y Enterprise x64 Microsoft Windows Server 2008 ediciones Web, Standard y Enterprise (x86 de 32 bits) Microsoft Windows Server 2008 ediciones Web, Standard, Enterprise y Datacenter (x64) **NOTA:** Al instalar Windows Server 2003 con Service Pack 1, tenga en cuenta los cambios de la configuración de seguridad de DCOM. Para obtener más información, consulte el artículo 903220 en el sitio web de asistencia técnica de Microsoft en **support.microsoft.com/kb/903220**.
Red Hat® Linux®	Enterprise Linux WS, ES y AS (versión 4) (x86 y x86_64) Enterprise Linux 5 (x86 y x86-64)
SUSE® Linux	Enterprise Server 9 con actualización 2 y actualización 3 (x86_64) Enterprise Server 10 (Gold) (x86_64).

Exploradores web admitidos

La tabla 1-2 presenta una lista de los exploradores web que se admiten como clientes del iDRAC.

Consulte el archivo léame del iDRAC y la *Guía de compatibilidad de Dell OpenManage Server Administrator* que se encuentra en el sitio web de asistencia Dell Support en **support.dell.com** para conocer información más reciente.

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

Tabla 1-2. Exploradores de web compatibles

Sistema operativo	Explorador de web admitido
Windows	Internet Explorer 6.0 (de 32 bits) con Service Pack 2 (SP2) para Windows XP y Windows 2003 R2 SP2 solamente Internet Explorer 7.0 para Windows Vista, Windows XP, Windows 2003 R2 SP2 y Windows Server 2008 solamente Mozilla Firefox 2.0 para Windows (consola Java vKVM/vMedia solamente)
Linux	Mozilla Firefox 1.5 en SUSE Linux (versión 10) solamente Mozilla Firefox 2.0 en Red Hat Enterprise Linux 4 y 5 (32 bits o 64 bits) y Suse Linux Enterprise Server 10 (32 bits o 64 bits)

Conexiones de acceso remoto admitidas

La tabla 1-3 muestra una lista de las funciones de conexión.

Tabla 1-3. Conexiones de acceso remoto admitidas

Conexión	Características
NIC de iDRAC	• Ethernet de 10 Mbps/100 Mbps/1 Gbps a través del puerto Gb Ethernet del CMC • Compatibilidad con DHCP • Notificación de sucesos de correo electrónico y capturas SNMP • Compatibilidad para el shell de comandos SM-CLP (Telnet o SSH) para operaciones como la configuración del iDRAC, el inicio de sistema, el restablecimiento, el encendido y los comandos de apagado • Compatibilidad para las utilidades de IPMI, como ipmitool e ipmishell

Puertos del iDRAC

La tabla 1-4 muestra una lista de los puertos en los que el iDRAC detecta las conexiones. La tabla 1-5 identifica los puertos que el iDRAC usa como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un iDRAC.

Tabla 1-4. Puertos en los que el iDRAC detecta servidores

Número de puerto	Función
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*, 3669*	Servicio de medios virtuales
3770*, 3771*	Servicio seguro de medios virtuales
5900*	Teclado y mouse de la redirección de consola
5901*	Vídeo de la redirección de consola
* Puerto configurable	

Tabla 1-5. Puertos de cliente de iDRAC

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 útiles

Además de esta *Guía del usuario*, los siguientes documentos proporcionan información adicional sobre la configuración y funcionamiento del iDRAC en el sistema:

- La ayuda en línea de iDRAC proporciona información sobre el uso de la interfaz web.
- La *Guía del usuario del firmware Dell del Chassis Management Controller* suministra información acerca del uso del controller que administra todos los módulos en el chasis que contiene su servidor PowerEdge.
- La *Guía del usuario de Dell OpenManage IT Assistant* contiene información sobre cómo usar IT Assistant.
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- La *Guía del usuario de Dell Update Packages* contiene información acerca de cómo obtener y usar los Dell Update Packages como parte de su estrategia de actualización del sistema.

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

- La *Guía de información del producto* contiene información importante sobre seguridad y normativas. La información sobre la garantía puede estar incluida en este documento o constar en un documento aparte.
- En los documentos *Guía de instalación del rack* e *Instrucciones de instalación del rack* incluidos con el rack se describe cómo instalar el sistema en un rack.
- En la *Guía de introducción* se ofrece una visión general sobre los componentes, la configuración y las especificaciones técnicas del sistema.
- En el *Manual del propietario del hardware* se proporciona información sobre las características del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.
- En la documentación del software de administración de sistemas se describen las funciones, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación del sistema operativo se describe cómo instalar (si es necesario), configurar y usar el software del sistema operativo.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- Algunas veces, con el sistema se incluyen actualizaciones que describen los cambios realizados en el sistema, en el software o en la documentación.

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

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

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

Esta sección contiene información sobre cómo establecer el acceso al iDRAC y configurar el entorno de administración para usar el iDRAC.

Antes de comenzar

Reúna los siguientes elementos antes de configurar el iDRAC:

- *Guía del usuario del firmware Dell del Chassis Management Controller*
- CD *Dell PowerEdge Installation and Server Management*
- CD *Dell Systems Management Consoles*
- CD *Dell PowerEdge Service and Diagnostic Utilities*
- CD *Dell PowerEdge Documentation*

Interfaces para configurar el iDRAC

Puede configurar el iDRAC a través de la utilidad de configuración del iDRAC, la interfaz web del iDRAC, la CLI de RACADM local o la CLI de SM-CLP. La CLI de RACADM local está disponible después haber instalado el sistema operativo y el software de administración de servidor Dell PowerEdge en el servidor administrado. La tabla 2-1 describe estas interfaces.

Para mayor seguridad, el acceso a la configuración iDRAC a través de la utilidad de configuración del iDRAC puede desactivarse con un comando RACADM (consultar Generalidades del subcomando RACADM) o desde la interfaz gráfica para el usuario (consultar Activación o desactivación del acceso a la configuración local).

AVISO: Si usa más de una interfaz de configuración al mismo tiempo, puede obtener resultados inesperados.

Tabla 2-1. Interfaces de configuración

Interfaz	Descripción
Configuración del iDRAC Utilidad	La utilidad de configuración del iDRAC se accede al momento de inicio y es útil cuando se instala un nuevo servidor PowerEdge. Úsela para configurar la red y las funciones básicas de seguridad, así como para habilitar otras funciones.
Interfaz web del iDRAC	La interfaz web del iDRAC es una aplicación de administración a la que se accede por medio de explorador y que se puede usar para administrar el iDRAC de manera interactiva y supervisar al servidor administrado. Es la interfaz principal para las tareas cotidianas, como la supervisión de la condición de sistema, la consulta del registro de sucesos del sistema, la administración de usuarios locales del iDRAC y la ejecución de la interfaz web del CMC y las sesiones de redirección de consola.
Interfaz web del CMC	Además de supervisar y administrar el chasis, la interfaz web del CMC se puede usar para ver el estado de un servidor administrado, configurar los valores de la red de iDRAC e iniciar, detener o restablecer el servidor administrado.
Panel LCD del chasis	El panel LCD en el chasis que contiene el iDRAC se puede usar para ver el estado general de los servidores en el chasis. Durante la configuración inicial del CMC, el asistente de configuración permite activar la configuración de DHCP del sistema de red del iDRAC.
RACADM local	La interfaz de línea de comandos de RACADM local se ejecuta en el servidor administrado. Se accede a ella a través del conmutador iKVM o de una sesión de redirección de consola iniciada desde la interfaz web de iDRAC. RACADM se instala en el servidor administrado cuando usted instala Dell OpenManage Server Administrator. Los comandos de RACADM proporcionan acceso a casi todas las funciones de iDRAC. Usted puede inspeccionar datos de sensor, anotaciones del registro de sucesos de sistema y el estado actual y los valores de configuración que se mantienen en el iDRAC. Usted puede cambiar los valores de configuración del iDRAC, administrar usuarios locales, activar y desactivar funciones y realizar acciones de alimentación como apagar o reiniciar el servidor administrado.
iVM-CLI	La interfaz de línea de comandos de medios virtuales del iDRAC (iVM-CLI) proporciona al servidor administrado acceso a los medios que se encuentran en la estación de administración. Es útil para desarrollar secuencias de comandos para instalar sistemas operativos en varios servidores administrados.
SM-CLP	SM-CLP es la implementación incorporada en el iDRAC del Protocolo de línea de comandos de administración de servidor (SM-CLP) del grupo de trabajo de administración de servidor. A la línea de comandos de SM-CLP se accede mediante un inicio de sesión en el iDRAC a través de Telnet o SSH. Los comandos de SM-CLP implementan un subconjunto útil de los comandos de RACADM local. Los comandos resultan útiles para la creación de secuencias de comando pues se pueden ejecutar desde la línea de comandos una estación de administración. La salida de los comandos se puede obtener en formatos bien definidos, incluso en XML, lo que facilita la creación de secuencias de comandos y la integración con las herramientas de informes y de administración existentes.

	Consulte Equivalencias de RACADM y SM-CLP para ver una comparación de los comandos de RACADM y SM-CLP.
IPMI	IPMI define una manera estándar en la que los subsistemas de administración incorporados, como el iDRAC, se comuniquen con otros sistemas incorporados y aplicaciones de administración. Usted puede usar la interfaz web del iDRAC, SM-CLP o los comandos de RACADM para configurar filtros de sucesos de plataforma (PEF) de IPMI y capturas de sucesos de plataforma (PET). Los filtros de sucesos de plataforma hacen que el iDRAC realice acciones seleccionadas (por ejemplo, que reinicie el servidor administrado) cuando detecta una condición. Las capturas de sucesos de plataforma indican al iDRAC que envíe correo electrónico o alertas de IPMI cuando detecte los sucesos o condiciones especificados. Usted también puede usar herramientas IPMI estándares como **ipmitool** e **ipmishell** con iDRAC cuando activa la IPMI en el LAN.

Tareas de configuración

Esta sección es una descripción general de las tareas de configuración de la estación de administración, el iDRAC y el servidor administrado. Las tareas a realizar incluyen la configuración del iDRAC para que se pueda usar de manera remota, la configuración de las características del iDRAC que usted desea usar, la instalación del sistema operativo en el servidor administrado y la instalación del software de administración en la estación de administración y el servidor administrado.

Las tareas de configuración que se pueden usar para realizar cada tarea se muestran en una lista bajo la tarea.

NOTA: Antes de realizar los procedimientos de configuración que aparecen en esta guía, el CMC y los módulos de E/S se deben instalar en el chasis y se deben configurar y, además, el servidor PowerEdge debe estar físicamente instalado en el chasis.

Configurar la estación de administración

Establezca una estación de administración mediante la instalación del software Dell OpenManage, un explorador web y otras utilidades de software.

- Consulte el apartado Configuración de la estación de administración.

Configurar el sistema de red de iDRAC

Active la red de iDRAC y configure las direcciones IP, la máscara de red, la puerta de enlace y las direcciones DNS.

NOTA: Para mayor seguridad, el acceso a la configuración iDRAC a través de la utilidad de configuración del iDRAC puede desactivarse con un comando RACADM (consultar Generalidades del subcomando RACADM) o desde la interfaz gráfica para el usuario (consultar Activación o desactivación del acceso a la configuración local).

NOTA: Si cambia la configuración de la red de iDRAC cerrará todas las conexiones actuales de red al iDRAC.

NOTA: La opción para configurar el servidor mediante el panel LCD *sólo* está disponible durante la configuración inicial del CMC. Una vez que el chasis está instalado, el panel LCD no se puede usar para reconfigurar el iDRAC.

NOTA: El panel LCD se puede usar para activar DHCP para configurar la red de iDRAC. Si desea asignar direcciones estáticas, deberá usar la utilidad de configuración del iDRAC o la interfaz web del CMC.

- Panel LCD del chasis: consulte la *Guía del usuario de firmware Dell Chasis Management Controller*.
- Utilidad de configuración del iDRAC: consulte LAN
- Interfaz web del CMC: consulte Configuración del sistema de red por medio de la interfaz web del CMC
- RACADM: consulte cfgLanNetworking

Configurar los usuarios de iDRAC

Configure los usuarios y permisos locales del iDRAC. El iDRAC tiene una tabla de dieciséis usuarios locales en el firmware. Usted puede establecer nombres de usuarios, contraseñas y funciones para estos usuarios.

- Utilidad de configuración del iDRAC (sólo configura al usuario administrativo): consulte Configuración de usuario de la LAN
- Interfaz web del iDRAC: consulte Cómo agregar y configurar usuarios de iDRAC
- RACADM: consulte Cómo agregar un usuario de iDRAC

Configurar Active Directory

Además de los usuarios locales de iDRAC, se puede usar Microsoft® Active Directory® para autenticar los inicios de sesión de los usuarios de iDRAC.

- Consulte el apartado Uso de iDRAC con Microsoft Active Directory.

Configurar la filtración de IP y el bloqueo de IP

Además de la autentificación de usuario, usted puede impedir los accesos no autorizados mediante el rechazo de los intentos de conexión de direcciones IP fuera de un rango definido y mediante el bloqueo temporal de las conexiones de direcciones IP donde la autentificación ha fallado varias veces dentro de un periodo configurable.

- Interfaz web del iDRAC: consulte Configuración de la filtración de IP y el bloqueo de IP
- RACADM: consulte Configuración de la filtración de IP (IpRange), "Configuración del bloqueo de IP"

Configurar los sucesos de plataforma

Los sucesos de plataforma ocurren cuando el iDRAC detecta una condición de advertencia o crítica de uno de los sensores del servidor administrado.

Configure los filtros de sucesos de plataforma (PEF) para elegir los sucesos que desea detectar, por ejemplo, el reinicio del servidor administrado, cuando se detecta un suceso.

- Interfaz web del iDRAC: consulte Configuración de los filtros de sucesos de plataforma (PEF)
- RACADM: consulte Configuración del PEF

Configure capturas de sucesos de plataforma (PET) para enviar notificaciones de alerta a una dirección IP, por ejemplo, a una estación de administración con el software IPMI o para enviar un correo electrónico a una dirección de correo electrónico específica.

- Interfaz web del iDRAC: consulte Configuración de capturas de suceso de plataforma (PET)
- RACADM: Configuración de la PET

Activación o desactivación del acceso de configuración local

El acceso a los parámetros de configuración como la configuración de red y los privilegios de usuario puede desactivarse. Una vez desactivados, la configuración persiste al reiniciar. El acceso de escritura de configuración está bloqueado tanto para el programa RACADM local como para la utilidad de configuración iDRAC (al reiniciar). El acceso web a los parámetros de configuración está libre y los datos de configuración siempre están disponibles para su visualización. Para información acerca de la interfaz web iDRAC, consulte Activación o desactivación del acceso a la configuración local. Para comandos de ajuste cfgRac, consulte cfgRacTuning.

Configuración de la comunicación en serie en la LAN

La comunicación en serie en la LAN (SOL) es una característica de IPMI que permite desviar las E/S del puerto serie del servidor administrado en la red. La comunicación en serie en la LAN activa la función de redirección de consola del iDRAC.

- Interfaz web del iDRAC: consulte Activación o desactivación del acceso a la configuración local
- Consulte también Uso de la redirección de consola con interfaz gráfica de usuario

Configurar los servicios del iDRAC

Active o desactive los servicios de red del iDRAC -como Telnet, SSH y la interfaz del servidor web- y reconfigure los puertos y otros parámetros de servicios.

- Interfaz web del iDRAC: consulte Configuración de los servicios de iDRAC
- RACADM: consulte Configuración de los servicios de Telnet y SSH del iDRAC por medio de RACADM local

Configuración de la capa de conexión segura (SSL)

Configurar SSL para el servidor web del iDRAC.

- Interfaz web del iDRAC: consulte Capa de conexión segura (SSL)
- RACADM: consulte cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload, sslcertview

Configurar los medios virtuales

Configure la función de medios virtuales para que pueda instalar el sistema operativo en el servidor PowerEdge. Los medios virtuales permiten que el servidor administrado tenga acceso a dispositivos de medios en la estación de administración o a imágenes ISO de CD/DVD que estén en un recurso compartido de red como si fueran dispositivos en el servidor administrado.

- Interfaz web del iDRAC: consulte Configuración y uso de medios virtuales
- Utilidad de configuración del iDRAC: consulte Medios virtuales

Instalación del software de servidor administrado

Instale el sistema operativo en el servidor PowerEdge mediante los medios virtuales y luego instale el software Dell OpenManage en el servidor PowerEdge administrado y configure la función de pantalla de último bloqueo.

- Redirección de consola: consulte Instalación del software en el servidor administrado
- iVM-CLI: consulte Uso de la utilidad de interfaz de línea de comandos de los medios virtuales

Configure el servidor administrado para usar la función de pantalla de último bloqueo

Configure el servidor administrado de modo que el iDRAC pueda capturar la imagen de la pantalla tras un bloqueo o falla general del sistema operativo.

- Servidor administrado: consulte Configuración del servidor administrado para capturar la pantalla de último bloqueo, Desactivación de la opción de reinicio automático de Windows

---

Configuración del sistema de red por medio de la interfaz web del CMC

NOTA: Debe contar con privilegios de administrador de configuración de chasis para definir la configuración de red de iDRAC desde la CMC.

NOTA: El usuario de la CMC predeterminado es **root** y la contraseña predeterminada es **calvin**.

NOTA: La dirección IP del CMC se puede encontrar en la interfaz web del iDRAC si se hace clic en **Sistema**→ **Acceso remoto**→ **CMC**. También puede abrir la interfaz web del CMC a partir de esta página.

1. Use el explorador web para iniciar sesión en la interfaz de usuario web del CMC mediante la URL con el formato https://<*dirección_IP_del_CMC*> o https://<*nombre_DNS_del_CMC*>.
2. Introduzca el nombre de usuario del CMC y la contraseña y haga clic en **Aceptar**.
3. Haga clic en el símbolo más (+) junto a **Chassis** (Chasis) en la columna izquierda y, a continuación, haga clic en **Servers** (Servidores).
4. Haga clic en **Configuración**→ **Implementar red**.
5. Active la LAN para el servidor seleccionando la casilla de marcación que se encuentra junto al servidor, bajo el encabezado **Activar LAN**.
6. Active o desactive IPMI sobre LAN marcando o desmarcando la casilla de verificación debajo del encabezado **Enable IPMI over LAN** (Activar IPMI sobre LAN).
7. Active o desactive DHCP para el servidor seleccionando o deseleccionando la casilla que se encuentra junto al servidor, bajo el encabezado **DHCP activado**.
8. Si DHCP está desactivado, introduzca la dirección IP estática, la máscara de red y la puerta de enlace predeterminada del servidor.
9. Haga clic en **Apply** (Aplicar) en la parte inferior de la página.

Visualización de las conexiones de red fabric de la tarjeta intermedia FlexAdress

El M1000e incluye Flexadress, un sistema de red multiestándar multinivel avanzado. FlexAddress permite el uso de nombres de red mundial y direcciones MAC (WWN/MAC) persistentes con chasis asignado para cada conexión de puerto de servidor administrada.

AVISO: Con el propósito de evitar errores que puedan llevar a incapacitar la energía en el servidor administrado, usted *debe* tener el tipo correcto de tarjeta intermedia para cada conexión de puerto y red fabric.

La configuración de la función FlexAddress se realiza usando la interfaz web de CMC. Para más información sobre la función FlexAddress y su configuración, consulte su *Guía del Usuario de firmware Dell del Chassis Management Controller versión 1.20.*.

Una vez que la función FlexAddress se ha activado y configurado para el gabinete, haga clic en **Sistema**→ **Propiedades**→ **WWN/MAC** para ver una lista de tarjetas intermedias instaladas, las redes fabric y puertos a los que están conectados, la ubicación del puerto de red fabric, el tipo de red fabric, y las direcciones MAC configuradas en el servidor o con asignación de chasis para cada puerto de tarjeta intermedia incorporada a Ethernet u opcional instalados.

Para ver una lista de las tarjetas intermedias instaladas, el tipo de tarjetas intermedias instaladas y si FlexAddress está configurada, haga clic en **Sistema**→ **Propiedades**→ **Resumen**.

Actualización del firmware del iDRAC

La actualización del firmware del iDRAC instala una nueva imagen de firmware en la memoria flash del iDRAC. Puede actualizar el firmware por medio de alguno de los métodos siguientes:

- El comando **load** de SM-CLP
- La interfaz web del iDRAC
- Dell Update Package (para Linux o Microsoft Windows)
- La utilidad de actualización del firmware del iDRAC de DOS
- La interfaz web del CMC (sólo si el firmware del iDRAC está dañado)

Descarga del firmware o el paquete de actualización

Descargue el firmware de **support.dell.com**. La imagen del firmware está disponible en varios formatos distintos a fin de admitir los distintos métodos de actualización que tiene a su disposición.

Para actualizar el firmware del iDRAC por medio de la interfaz web del iDRAC o de SM-CLP, o para recuperar el iDRAC mediante la interfaz web del CMC, descargue la imagen binaria que viene comprimida como archivo de extracción automática.

Para actualizar el firmware del iDRAC desde el servidor administrado, descargue el Dell Update Package (DUP) para el sistema operativo que se ejecuta en el servidor cuyo iDRAC va a actualizar.

Para actualizar el firmware del iDRAC por medio de la utilidad de actualización del firmware del iDRAC de DOS, descargue la utilidad de actualización y la imagen binaria, que vienen comprimidos en archivos de extracción automática.

Ejecutar la actualización del firmware

NOTA: Cuando la actualización de firmware del iDRAC comienza, todas las sesiones existentes en el iDRAC se desconectan y no se permitirán nuevas sesiones hasta que el proceso de actualización haya terminado.

NOTA: Los ventiladores del chasis funcionan al 100% durante la actualización de firmware del iDRAC. Cuando la actualización concluya, se reanudará la regulación normal de la velocidad de los ventiladores. Éste es el comportamiento normal y fue diseñado para proteger el servidor contra sobrecalentamientos durante el periodo en que no se puede enviar información del sensor al CMC.

Para usar un Dell Update Package para Linux o Microsoft Windows, ejecute el DUP específico para el sistema operativo en el servidor administrado.

Cuando se usa el comando **load** de SM-CLP, coloque la imagen binaria de firmware en un directorio donde un servidor TFTP (Protocolo de transferencia de archivos trivial) pueda tenerlo a disposición del iDRAC. Consulte el apartado Actualización del firmware del iDRAC por medio de SM-CLP.

Cuando use la interfaz web del iDRAC o la interfaz web del CMC, coloque la imagen binaria del firmware en un disco al que se pueda acceder desde la estación de administración en la que usted ejecuta la interfaz web. Consulte el apartado Actualización del firmware del iDRAC.

NOTA: La interfaz web del iDRAC también permite restablecer la configuración predeterminada de fábrica del iDRAC.

Usted puede usar la interfaz web del CMC para actualizar el firmware *sólo* cuando el CMC detecte que el firmware del iDRAC está dañado, como ocurriría si el progreso de la actualización de firmware del iDRAC se interrumpe antes de que termine. Consulte el apartado Recuperación del firmware del iDRAC por medio del CMC.

NOTA: Después de que el CMC actualiza el firmware del iDRAC, el iDRAC genera nuevas claves SHA1 y MD5 para el certificado SSL. Como las claves son diferentes que las claves en el explorador web abierto, todas las ventanas del explorador que están conectadas al iDRAC deben cerrarse después de finalizar la actualización del firmware. Si las ventanas del explorador no se cierran, se verá un mensaje de error **Certificado inválido.**

NOTA: Si está realizando una actualización de su firmware iDRAC de la versión 1.20 a una versión anterior, debe eliminar el complemento existente del explorador Internet Explorer ActiveX de cualquier Management Station basada en Windows para permitir que el firmware instale una versión compatible del complemento ActiveX. Para eliminar un complemento ActiveX, navegue hasta **c:\WINNT\Archivos de programa descargados** y elimine el archivo **DELL IMC KVM Viewer**.

Uso de la utilidad de actualización de DOS

Para actualizar el firmware del iDRAC por medio de la utilidad de actualización de DOS, inicie al servidor administrado en DOS y ejecute el comando **idrac16d**. La sintaxis del comando es:

```
idrac16d [-f] [-i=<nombre_de_archivo>] [-l=<archivo_de_registro>]
```

Cuando se ejecuta sin agregar opciones, el comando **idrac16d** actualiza el firmware del iDRAC con el archivo de imagen de firmware **firmimg.imc** en el directorio actual.

Las opciones son las siguientes:

`-f`: fuerza la actualización. La opción `-f` se puede usar para *degradar* el firmware a una imagen anterior.

`-i=<nombre_de_archivo>`: especifica el nombre del archivo que contiene la imagen de firmware. Esta opción es necesaria cuando el nombre de archivo predeterminado del firmware, **firmimg.imc**, ha sido cambiado.

`-l=<archivo_de_registro>`: registra la salida de la actividad de actualización. Esta opción se usa para depuración.

AVISO: Si usted introduce argumentos incorrectamente con el comando **idrac16d** o añade la opción `-h`, tal vez note una opción adicional, `-nopresconfig` en el mensaje de salida sobre su uso. Esta opción se usa para actualizar el firmware sin conservar la información de configuración. Usted **no** debe usar esta opción, pues *elimina* toda la información existente de configuración del iDRAC, por ejemplo, las direcciones IP, los usuarios y las contraseñas.

Verificación de la firma digital

La firma digital se usa para autenticar la identidad del firmante de un archivo y para certificar que el contenido original del archivo no ha sido modificado desde que se firmó.

Si aún no lo tiene instalado en el sistema, deberá instalar el Resguardo de privacidad GNU (GPG) para verificar firmas digitales. Para usar el procedimiento de verificación estándar, realice los pasos a continuación:

1. Descargue la clave GnuPG pública de Linux de Dell, si aún no la tiene de la siguiente manera: visite **lists.us.dell.com** y haga clic en el vínculo **Dell Public GPG key (Clave GPG pública de Dell)**. Guarde el archivo en el sistema local. El nombre predeterminado es **linux-security- publickey.txt**.

2. Importe la clave pública a la base de datos de confianza de GPG mediante la ejecución del comando siguiente:

   ```
   gpg --import <Nombre de archivo de clave pública>
   ```

NOTA: Para completar este proceso, deberá tener la clave privada.

3. Para evitar una advertencia de clave no confiable, cambie el nivel de confianza de la clave GPG pública de Dell.

   e. Escriba el siguiente comando:

   ```
   gpg --edit-key 23B66A9D
   ```

   f. Dentro del editor de claves GPG, escriba `fpr`. Aparece el mensaje siguiente:

   ```
   pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group) <linux-security@dell.com>
   Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
   ```

   Si la huella digital de la clave importada es igual a la anterior, usted tiene una copia correcta de la clave.

   g. Mientras aún está en el editor de claves GPG, escriba `trust`. Aparecerá el siguiente menú:

   ```
   Decida el nivel de confianza que otorga a este usuario a fin de verificar correctamente las claves de otros usuarios (revisando
   pasaportes, comprobando huellas digitales de distintas fuentes, etc.)


     1 = I don't know or won't say
     2 = I do NOT trust
     3 = I trust marginally
     4 = I trust fully
     5 = I trust ultimately
     m = back to the main menu

   Your decision?
   ```

   h. Escriba `5` <Entrar>. Aparecerá la siguiente petición:

   ```
   Do you really want to set this key to ultimate trust? (y/N)
   ```

   i. Escriba `y` <Entrar> para confirmar su elección.

   j. Escriba `quit` <Entrar> para salir del editor de claves GPG.

   Debe importar y validar la clave pública sólo una vez.

4. Obtenga el paquete que necesita, por ejemplo, el DUP de Linux o el archivo de extracción automática, y el archivo de firma asociado del sitio web de asistencia Dell Support en **support.dell.com/support/downloads**.

   NOTA: Cada paquete de actualización de Linux tiene un archivo de firma independiente, el cual aparece en la misma página web que el paquete de actualización. Usted necesita el paquete de actualización y el archivo de firma relacionado para la verificación. De manera predeterminada, el archivo de firma tiene el mismo nombre que el archivo del DUP, con la extensión **.sign**. Por ejemplo, si un DUP Linux se llama **PEM600_BIOS_LX_2.1.2.BIN**, el nombre del archivo del firmware de firma es **PEM600_BIOS_LX_2.1.2.BIN.sign**. La imagen del firmware del iDRAC también tiene un archivo **.sign** asociado, que se incluye en el archivo de extracción automática con la imagen del firmware. Para descargar los archivos, haga clic con el botón derecho del mouse en el vínculo de descarga y use la opción **Guardar destino como...** del archivo.

5. Verifique el paquete de actualización:

   ```
   gpg --verify <nombre de archivo de firma del paquete de actualización de Linux> <nombre de archivo del paquete de actualización de Linux>
   ```

El ejemplo siguiente ilustra los pasos a seguir para verificar un paquete de actualización del PowerEdge M600 BIOS:

1. Descargue los dos archivos siguientes de **support.dell.com**:

   - PEM600_BIOS_LX_2.1.2.BIN.sign
   - PEM600_BIOS_LX_2.1.2.BIN.sign

2. Importe la clave pública mediante la ejecución de la línea de comandos siguiente:

   ```
   gpg --import <linux-security-publickey.txt>
   ```

Aparecerá el siguiente mensaje de salida:

```
gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed
gpg: Total number processed: 1
gpg: unchanged: 1
```

3. Establezca el nivel de confianza de GPG para la clave pública de Dell. si no lo ha hecho aún.

   a. Escriba el comando siguiente:

   ```
   gpg --edit-key 23B66A9D
   ```

   b. En la petición de comandos, escriba los comandos siguientes:

   ```
   fpr
   trust
   ```

   c. Escriba 5 <Entrar> para elegir `confío plenamente` en el menú.

   d. Escriba y <Entrar> para confirmar su elección.

   e. Escriba `quit` <Entrar> para salir del editor de claves GPG.

   Esto completa la validación de la clave pública de Dell.

4. Verifique la firma digital del paquete del BIOS de PEM600 mediante la ejecución del comando siguiente:

   ```
   gpg --verify PEM600_BIOS_LX_2.1.2.BIN.sign PEM600_BIOS_LX_2.1.2.BIN
   ```

   Aparecerá el siguiente mensaje de salida:

   ```
   gpg: Firma realizada Vie Jul 11 15:03:47 2008 CDT usando clave DSA ID 23B66A9D
   gpg: Buena firma de "Dell, Inc. (grupo del producto) <linux-security@dell.com>"
   ```

   NOTA: Si no ha validado la clave como se muestra en paso 3, recibirá mensajes adicionales:

   ```
   gpg: ADVERTENCIA: Esta clave no está certificada con una firma confiable.
   gpg: No hay indicación de que la firma pertenezca al propietario.
   Huella digital de clave primaria: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
   ```

Limpiar el caché del explorador

Para poder usar las funciones del último iDRAC, deberá limpiar el caché del explorador para eliminar cualquier página *antigua* que podría estar guardada en el sistema.

Internet Explorer

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas** y después en **Opciones de Internet**.

   Aparece la ventana **Opciones de Internet**.

3. Haga clic en la ficha **General**.
4. En **archivos temporales de Internet**, haga clic en **Eliminar archivos**.

   Ahora aparece la ventana **Eliminar archivos**.

5. Haga clic para seleccionar **Eliminar todo el contenido offline** y después haga clic en **Aceptar**.
6. Haga clic en Aceptar para cerrar la ventana **Opciones de Internet**.

Firefox

1. Inicie Firefox.
2. Haga clic en **Editar**→ **Preferencias**.
3. Haga clic en la ficha **Privacidad**.

4. Haga clic en **Limpiar caché ahora**.
5. Haga clic en **Close** (Cerrar).

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la estación de administración

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Una estación de administración es un equipo que se usa para supervisar y administrar los servidores PowerEdge y otros módulos en el chasis. Esta sección describe la instalación del software y las tareas de configuración que preparan una estación de administración para trabajar con el iDRAC. Antes de que comience a configurar el iDRAC, siga los procedimientos en esta sección para asegurarse que ha instalado y configurado las herramientas que necesitará.

Pasos de configuración de la estación de administración

Para configurar la estación de administración, realice los pasos siguientes:

1. Configure la red de la estación de administración.
2. Instale y configure un explorador de web admitido.
3. Instale Java Runtime Environment (JRE) (opcional para Windows).
4. Instale clientes de SSH o Telnet, de ser necesario.
5. Instale a un servidor TFTP, de ser necesario.
6. Instale Dell OpenManage IT Assistant (opcional).

Requisitos de la red de la estación de administración

Para tener acceso al iDRAC, la estación de administración debe estar en la misma red que el puerto de conexión RJ45 del CMC que está etiquetado como "GB1". Es posible aislar la red del CMC de la red en la que se encuentra el servidor administrado, de modo que la estación de administración pueda tener el acceso de LAN al iDRAC, pero no al servidor administrado.

Por medio de la función de redirección de consola del iDRAC (consulte Uso de la redirección de consola con interfaz gráfica de usuario), se puede tener acceso a la consola del servidor administrado aun cuando no se tenga acceso de red a los puertos del servidor. Usted también puede realizar varias funciones de administración en el servidor administrado, como el reinicio del equipo, mediante los servicios del iDRAC. Sin embargo, para tener acceso a red y a los servicios de aplicación que se encuentran en el servidor administrado, es posible que necesite tener una tarjeta adicional de interfaz de red en el equipo de administración.

Configuración de un explorador de web admitido

Las secciones siguientes contienen instrucciones para configurar los exploradores web admitidos para su uso con la interfaz web del iDRAC. Para ver una lista de los exploradores de web admitidos, consulte Exploradores web admitidos.

Abrir el explorador web

La interfaz web iDRAC está diseñada para verse en un explorador web compatible con una resolución de pantalla mínima de 800 pixeles de ancho por 600 pixeles de alto. Para poder visualizar la interfaz y acceder a todas las funciones, asegúrese de que su resolución esté configurada al menos en 800 por 600 pixeles y/o cambie el tamaño de su explorador, según sea necesario.

NOTA: En algunas situaciones, con frecuencia durante la primera sesión después de una actualización de firmware, los usuarios de Internet Explorer 6 verán un mensaje que dice **Finalizado, con errores** en la barra de estado del explorador junto con una página parcialmente renderizada en la ventana principal del explorador. Este error también puede ocurrir si está experimentando problemas de conectividad. Este es un problema conocido con Internet Explorer 6. Cierre el explorador y vuelva a comenzar.

Configuración del explorador web para conectarse a la interfaz web

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

Para configurar el explorador web Internet Explorer para acceder a un servidor proxy, realice los pasos a continuación:

1. Abra una ventana del explorador web.
2. Haga clic en **Herramientas** y haga clic en **Opciones de Internet**.

   Aparece la ventana **Opciones de Internet**.

   NOTA: Las diferentes versiones de Internet Explorer tienen diferentes niveles de seguridad predeterminados. Para asegurarse de que su sistema funcione de forma correcta, haga clic en la ficha **Avanzado** y verifique que **Permitir instalar por demanda (otro)**, **Permitir extensiones de explorador de terceros**, **Permitir Sun Java** y **Usar SSL 3.0** estén seleccionados (los nombres pueden variar dependiendo de la versión). Si realiza cambios a estas configuraciones, reinicie el Internet Explorer.
3. 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 servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.
6. Haga clic dos veces en **Aceptar**.

Cómo agregar el iDRAC a la lista de dominios de confianza

Al acceder a la interfaz web de iDRAC a través del explorador web, es posible que se le pida que agregue la dirección IP de iDRAC a la lista de dominios de confianza, si dicha dirección IP no figura en la lista. Al terminar, haga clic en **Actualizar** o vuelva a iniciar el explorador web para establecer una conexión con la interfaz web de iDRAC.

Cómo ver las versiones traducidas de la interfaz web

La interfaz web del iDRAC es compatible con los siguientes idiomas de sistema operativo:

- Inglés (en-us)
- Francés (fr)
- Alemán (de)
- Español (es)
- Japonés (ja)
- Chino simplificado (zh-cn)

Los identificadores ISO en paréntesis denotan la variantes de idiomas específicos que son compatibles. El uso de la interfaz con otros dialectos o idiomas no es compatible y puede no funcionar como se desea. Para algunos idiomas compatibles, es posible que sea necesario ajustar el tamaño de la ventana del explorador a 1024 pixeles de ancho para visualizar todas las funciones.

La interfaz web iDRAC está diseñada para funcionar con teclados localizados para las variantes de idiomas específicos mencionados anteriormente. Algunas funciones de la interfaz web iDRAC, como la Redirección de consola, pueden requerir pasos adicionales para aceptar algunas funciones/letras. Para más detalles sobre cómo usar su teclado localizado en estos casos, consulte Uso de Video Viewer. El uso de otros teclados no es compatible y puede causar problemas inesperados.

Internet Explorer 6.0 (Windows)

Para ver una versión traducida de la interfaz web de iDRAC en Internet Explorer, realice los pasos a continuación:

1. Haga clic en el menú **Herramientas** y seleccione **Opciones de Internet**.
2. En la ventana **Internet Options** (Opciones de Internet), haga clic en **Languages** (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. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.
7. Haga clic en **OK** (Aceptar).

Firefox 1.5 (Linux)

Para ver una versión traducida de la interfaz web de iDRAC en Firefox 1.5, realice los pasos a continuación:

1. Haga clic en **Editar**→ **Preferencias** y luego haga clic en la ficha **Opciones avanzadas**.
2. En la sección **Idioma**, haga clic en **Elegir**.
3. Haga clic en **Seleccionar un idioma para agregar...**.
4. Seleccione un idioma admitido y haga clic en **Agregar**.
5. Seleccione el idioma de su elección y haga clic en **Subir** para subir el idioma al inicio de la lista.
6. En el menú Idiomas, haga clic en **Aceptar**.
7. Haga clic en **OK** (Aceptar).

Firefox 2.0 (Linux o Windows)

Para ver una versión traducida de la interfaz web de iDRAC en Firefox 2.0, realice los pasos a continuación:

1. Haga clic en **Herramientas**→ **Opciones** y después haga clic en la ficha **Avanzado**.
2. En **Idioma** haga clic en **Seleccionar**.

   Aparecerá la ventana de **Idiomas**.
3. En el menú desplegable **Seleccionar un idioma para añadir...**, haga clic para seleccionar un idioma compatible y después haga clic en **Agregar**.
4. Haga clic para seleccionar su idioma preferido y después haga clic en **Mover hacia arriba** hasta que el idioma aparezca en primer lugar en la lista.
5. Haga clic en **Aceptar** para cerrar la ventana **Idiomas**.
6. Haga clic en **Aceptar** para cerrar la ventana **Idiomas**.

Cómo establecer la configuración regional en Linux

El visor de redirección de consola requiere un conjunto de caracteres UTF-8 para mostrarse correctamente. Si la pantalla no es legible, revise la configuración local y, si es necesario, restablezca el conjunto de caracteres.

Los pasos siguientes muestran cómo establecer el conjunto de caracteres en un cliente Red Hat® Enterprise Linux® con una interfaz gráfica de usuario en chino simplificado:

1. Abra una ventana de terminal de comandos.
2. Escriba locale y presione <Entrar>. Aparecerá un mensaje de salida parecido al siguiente:

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

3. Si los valores incluyen "zh_CN.UTF-8", no será necesario hacer cambios. Si los valores no incluyen "zh_CN.UTF-8", vaya al paso 4.
4. Modifique el archivo **/etc/sysconfig/i18n** con un editor de textos.

5. En el archivo, aplique los cambios siguientes:

   Anotación actual:

   ```
   LANG=&amp;quot;zh_CN.GB18030&amp;quot;
   SUPPORTED=&amp;quot;zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh&amp;quot;
   ```

   Anotación actualizada:

   ```
   LANG=&amp;quot;zh_CN.UTF-8&amp;quot;
   SUPPORTED=&amp;quot;zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh&amp;quot;
   ```

6. Cierre sesión y después inicie sesión en el sistema operativo.

Cuando cambie de cualquier otro idioma, compruebe este ajuste sigue siendo válido. Si no es así, repita este procedimiento.

Desactivación de la función de lista blanca en Firefox

Firefox tiene una función de seguridad de "lista blanca" que requiere permiso del usuario para instalar complementos para cada sitio distinto que aloje un complemento. Cuando está activada, la función de lista blanca requiere que se instale un visor de redirección de consola por cada iDRAC que usted visite, aunque las versiones del visor sean idénticas.

Para desactivar la función de lista blanca y evitar la instalación innecesaria de complementos, realice los pasos a continuación:

1. Abra una ventana del explorador de web Firefox.

2. En el campo de dirección, escriba `about:config` y presione <Entrar>.

3. En la columna **Nombre de la preferencia**, localice **xpinstall.whitelist.required** y haga clic en éste.

   Los valores de **Nombre de la preferencia**, **Estado**, **Tipo** y **Valor** cambiarán a negritas. El valor **Estado** cambia a **establecido por el usuario** y el valor de **Valor** cambia a **false**.

4. En la columna **Nombre de la preferencia**, localice **xpinstall.enabled**.

   Asegúrese que **Valor** sea **true**. Si no lo es, haga doble clic en **xpinstall.enabled** para cambiar el **Valor** a **true**.

Instalación de Java Runtime Environment (JRE)

NOTA: Si usa el explorador Internet Explorer, se ofrece un control ActiveX para el visor de consola. También se puede usar el visor de consola de Java con Internet Explorer si instala JRE y configura el visor de consola en la interfaz web del iDRAC antes de ejecutar el visor. Para obtener más información, consulte el apartado Configuración de la redirección de consola en la interfaz web del iDRAC.

Usted puede optar por usar el visor de Java antes de ejecutar el visor.

Si usa el explorador Firefox deberá instalar JRE (o un paquete de desarrollo de Java [JDK]) para usar la función de redirección de consola. El visor de consola es una aplicación de Java que se descarga en la estación de administración de la interfaz web del iDRAC y después se ejecuta con Java Web Start en la estación de administración.

Visite **java.sun.com** para instalar JRE o JDK. Se recomienda la versión 1.6 (Java 6.0) o versiones superiores.

El programa Java Web Start se instala automáticamente junto con el JRE o JDK. El archivo **jviewer.jnlp** se descarga a su escritorio y un cuadro de diálogo le pregunta qué acción realizar. Puede ser necesario asociar el tipo de extensión .jnlp con la aplicación Java Web Start en su explorador. De otro modo, elija la opción de **Abrir con** y después seleccione la aplicación javaws, que se encuentra en el subdirectorio bin del directorio de instalación de JRE.

NOTA: Si el tipo de archivo .jnlp no está asociado con Java Web Start después de instalar JRE o JDK, puede configurar la asociación manualmente. Para Windows (**javaws.exe**) haga clic en **Inicio**→ **Panel de control**→ **Apariencia y temas**→ **Opciones de carpeta**. En la ficha **Tipos de archivos**, marque .jnlp en **Tipos de archivo registrados** y después haga clic en **Cambiar**. Para Linux (**javaws**), inicie Firefox y después haga clic en **Editar**→ **Preferencias**→ **Descargas** y después haga clic en **Acciones de visualización y edición**.

Para Linux, una vez que ha instalado JRE o JDK, agregue una ruta de acceso al directorio bin Java al frente de su RUTA DE ACCESO del sistema. Por ejemplo, si Java está instalado en /usr/java, agregue la siguiente línea a su local.bashrc o /etc/profil:

```
PATH=/usr/java/bin:$PATH; export PATH
```

NOTA: Es posible que los archivos ya contengan líneas de modificación de RUTA DE ACCESO. Asegúrese de que la información de ruta de acceso no cree conflictos.

Instalación de clientes Telnet o SSH

De manera predeterminada, el servicio Telnet del iDRAC está desactivado y el servicio SSH está activado. Como Telnet es un protocolo inseguro, sólo debe usarse cuando no se puede instalar un cliente SSH o la conexión de red tiene otro tipo de seguridad.

NOTA: Sólo puede haber una conexión Telnet o SSH activa con el iDRAC a la vez. Cuando haya una conexión activa, se rechazarán los demás intentos de conexión.

Telnet con iDRAC

Telnet se incluye en los sistemas operativos Microsoft® Windows® y Linux y se puede ejecutar desde un shell de comandos. También puede optar por instalar un cliente Telnet comercial o gratuito con más funciones prácticas de la versión estándar que se incluye en el sistema operativo.

Si la estación de administración está ejecutando Windows XP o Windows 2003, es posible que tenga un problema con los caracteres en las sesiones Telnet de iDRAC. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla <Entrar> no responde y no aparece la petición de contraseña.

Para resolver este problema, descargue la revisión (hotfix) 824810 del sitio web de asistencia técnica de Microsoft en **support.microsoft.com**. Consulte el artículo 824810 de Microsoft Knowledge Base para obtener más información.

Configuración de la tecla de retroceso para la sesión de Telnet

El uso de la tecla <Retroceso> puede producir resultados inesperados, según el cliente de Telnet. Por ejemplo, la sesión puede mostrar el eco ^h. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux se pueden configurar para usar la tecla <Retroceso>.

Para configurar los clientes Telnet de Microsoft para que puedan usar la tecla <Retroceso>, realice los pasos a continuación:

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

   `telnet`

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En 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>, realice los pasos a continuación:

1. Abra una petición de comandos y escriba:

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

   `telnet`

SSH con iDRAC

Secure Shell (SSH) es una conexión de línea de comandos con las mismas capacidades que una sesión Telnet, pero con negociación de sesión y cifrado para mejorar la seguridad. El iDRAC admite la versión 2 de SSH con autentificación de contraseña. SSH está activado en el iDRAC de manera predeterminada.

Se puede usar PuTTY (en Windows) u OpenSSH (en Linux) en una estación de administración para conectarse al iDRAC del servidor administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente de **ssh** envía un mensaje de error. El texto del mensaje está en función del cliente y no es controlado por el iDRAC.

NOTA: OpenSSH se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. La ejecución de OpenSSH en la petición de comandos de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

Sólo se admite una sesión de Telnet o de SSH en un momento dado. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se describe en Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC.

La implementación de SSH del iDRAC admite varios esquemas de criptografía, según se muestra en la tabla 3-1.

NOTA: No se admite SSHv1.

Tabla 3-1. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS 512:1024 bits (aleatorios) según la especificación NIST

Criptografía simétrica	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Integridad de mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autenticación	• Contraseña

Instalación de un servidor TFTP

NOTA: Si usa únicamente la interfaz web del iDRAC para transferir certificados de SSL y cargar nuevo firmware al iDRAC, no necesita un servidor TFTP.

El Protocolo de transferencia de archivos trivial (TFTP) es una forma simplificada del Protocolo de transferencia de archivos (FTP). Se usa con las interfaces de línea de comandos de SM-CLP y RACADM para transferir archivos al iDRAC y desde el mismo.

Las únicas ocasiones en las que necesita copiar archivos hacia el iDRAC y desde el mismo son cuando actualiza el firmware del iDRAC o cuando instala certificados en el iDRAC. Si decide usar SM-CLP o RACADM cuando realice estas tareas, deberá tener un servidor TFTP funcionando en un equipo al que el iDRAC pueda tener acceso por medio del número de IP o del nombre DNS.

Puede usar el comando **netstat -a** en los sistemas operativos Windows o Linux para determinar si ya hay un servidor TFTP activo. El puerto 69 es el puerto predeterminado de TFTP. Si no hay un servidor funcionado, usted tiene las siguientes opciones:

- Encuentre otro equipo en la red que ejecute un servicio TFTP
- Si usa Linux, instale un servidor TFTP a partir de su distribución
- Si usa Windows, instale un servidor TFTP comercial o gratuito

---

Instalación de Dell OpenManage IT Assistant

El sistema incluye el paquete de software Dell OpenManage System Management. Este paquete incluye, entre otros, los siguientes componentes:

- CD *Dell Systems Management Consoles*: contiene todos los productos más recientes de consola de administración de sistemas Dell, incluso Dell OpenManage IT Assistant.
- CD *Dell PowerEdge Service and Diagnostic Utilities*: proporciona las herramientas necesarias para configurar el sistema e incluye el firmware, los diagnósticos y los controladores optimizados por Dell para el sistema.
- CD *Dell PowerEdge Documentation*: ayuda a mantenerse actualizado con la documentación para sistemas, productos de software para la administración de sistemas, periféricos y controladores RAID.
- Sitio web de asistencia Dell Support y archivos léame: consulte los archivos léame y el sitio web de asistencia Dell Support en la dirección **support.dell.com** para ver la información más reciente de los productos Dell.

Use el CD *Dell System Management Consoles* para instalar el software de consola de administración, incluso Dell OpenManage IT Assistant, en la estación de administración. Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida*.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del servidor administrado

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Esta sección describe las tareas para configurar el servidor administrado a fin de mejorar las capacidades de administración remota. Estas tareas incluyen la instalación del software Dell OpenManage Server Administrator y la configuración del servidor administrado para capturar la pantalla de último bloqueo.

Instalación del software en el servidor administrado

El software de administración de Dell incluye los siguientes componentes:

- CLI de RACADM local: permite configurar y administrar el iDRAC a partir del sistema administrado. Es una herramienta potente tareas de configuración y administración de secuencias de comando.
- Se requiere que Server Administrator use la función de pantalla de último bloqueo del iDRAC.
- Server Administrator: una interfaz web que permite administrar el sistema remoto desde un host remoto en la red.
- Server Administrator Instrumentation Service: proporciona acceso a información detallada sobre fallas y rendimiento recopilada por agentes de administración de sistemas estándar de la industria y que hace posible la administración remota de sistemas supervisados, incluso acciones de apagado, arranque y seguridad.
- Servicio Storage Management de administración de servidor: brinda información sobre administración de almacenamiento en una vista gráfica integrada.
- Registros de Server Administrator: muestran registros de los comandos recibidos o enviados por el sistema, los sucesos de hardware supervisados, los sucesos de la POST y las alertas del sistema. Los registros se pueden ver en la página de inicio, imprimir o guardar como informes y enviarse por correo electrónico a un contacto de servicio designado.

Use el CD *Dell PowerEdge Installation and Server Management* para instalar Server Administrator. Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida*.

Configuración del servidor administrado para capturar la pantalla de último bloqueo

El iDRAC puede capturar la pantalla de último bloqueo para que usted pueda verla en la interfaz web a fin de ayudar a solucionar la causa del bloqueo del sistema administrado. Siga estos pasos para activar la función de pantalla de último bloqueo.

1. Instalación del software de servidor administrado. Para obtener más información acerca de cómo instalar el software de servidor administrado, consulte la *Guía del usuario de Server Administrator*.

2. Si usted ejecuta un sistema operativo Microsoft® Windows®, asegúrese que la función de reinicio automático esté deseleccionada en la **Configuración de inicio y recuperación de Windows**. Consulte el apartado Desactivación de la opción de reinicio automático de Windows.

3. Active la pantalla de último bloqueo (desactivada de manera predeterminada) en la interfaz web del iDRAC.

   Para activar la pantalla de último bloqueo en la interfaz web del iDRAC, haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**→ **Servicios** y luego seleccione la casilla **Activar** que se encuentra bajo del encabezado Configuración del agente de recuperación automática de sistema.

   Para activar la pantalla de último bloqueo por medio de RACADM local, abra una ventana de símbolo del sistema en el sistema administrado y escriba el siguiente comando:

   ```
   racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
   ```

4. En la interfaz web de Server Administrator, active el temporizador de **Recuperación automática** y establezca la acción de **Recuperación automática** como **Restablecer**, **Apagar** o **Ciclo de encendido**.

   Para obtener información sobre cómo configurar el temporizador de **Recuperación automática**, consulte la *Guía del usuario de Server Administrator*. Para asegurarse que la pantalla de último bloqueo se pueda guardar, el temporizador de **Recuperación automática** se deberá establecer en 60 segundos. El valor predeterminado es de 480 segundos.

   La pantalla de último bloqueo no estará disponible cuando la acción de **Recuperación automática** se establezca en **Apagar** o **Ciclo de encendido** si el servidor administrado está apagado.

Desactivación de la opción de reinicio automático de Windows

Para asegurarse de que el iDRAC pueda capturar la pantalla de último bloqueo, desactive la opción **Reinicio automático** en los servidores administrados que ejecutan Microsoft Windows Server® o Windows Vista®.

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.
2. Haga clic en la ficha **Opciones avanzadas**.
3. En **Inicio y recuperación**, haga clic en **Configuración**.
4. Deseleccione la casilla **Reiniciar automáticamente**.
5. Haga clic dos veces en **Aceptar**.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del iDRAC por medio de la interfaz web

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

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

La mayoría de las tareas de configuración de interfaz web también se pueden realizar con comandos de RACADM local o con comandos de SM-CLP.

Los comandos de RACADM local se ejecutan desde el servidor administrado. Para obtener más información sobre RACADM local, consulte Uso de la interfaz de línea de comandos de RACADM local.

Los comandos de SM-CLP se ejecutan en un shell al que se puede tener acceso de manera remota con una conexión Telnet o SSH. Para obtener más información sobre SM-CLP, consulte Uso de la interfaz de línea de comandos de SM-CLP de iDRAC.

Acceso a la interfaz web

Para acceder a la interfaz web de iDRAC, realice los pasos a continuación:

1. Abra una ventana del explorador web compatible.

   Para obtener más información, consulte el apartado Exploradores web admitidos.

2. En el campo **Dirección**, escriba `https://<Dirección_IP_del_iDRAC>` y presione <Entrar>.

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

   `https://<dirección_IP_de_iDRAC>:<número_de_puerto>`

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

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

Conexión

Puede iniciar sesión como usuario del iDRAC o como usuario de Microsoft® Active Directory®. El nombre predeterminado y la contraseña son **root** y **calvin**, respectivamente.

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

Para conectar, realice los pasos siguientes:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes valores:

   - Su nombre de usuario de iDRAC.

     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 *<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**, introduzca la contraseña de usuario del iDRAC o la contraseña de usuario de Active Directory. Las contraseñas distinguen entre mayúsculas y minúsculas.

3. Haga clic en **Aceptar** o presione <Entrar>.

Desconexión

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 aparecerá a menos que usted haya iniciado sesión.

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

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

Uso de múltiples fichas y ventanas en el explorador

Las distintas versiones de exploradores de web muestran diferentes comportamientos al abrir nuevas fichas y ventanas. Cada ventana es una nueva sesión, mientras que cada ficha no lo es. Microsoft Internet Explorer 6 no admite fichas; por lo tanto, cada ventana que se abre en el explorador es una sesión nueva de la interfaz web iDRAC. Internet Explorer 7 tiene la opción de abrir fichas así como también ventanas. Cada ficha hereda las características de la ficha abierta más recientemente. Por ejemplo, si un usuario inicia sesión con los privilegios de Usuario avanzado en una ficha y después inicia sesión como Administrador en otra ficha, ambas fichas abiertas tendrán privilegios de Administrador. Cerrar una ficha finaliza todas las fichas de interfaz web iDRAC.

El comportamiento de las fichas y las ventanas en Firefox es el mismo que en Internet Explorer 7.

Configuración del NIC del iDRAC

Esta sección supone que el iDRAC ya ha sido configurado y se puede tener acceso al mismo en la red. Consulte Configurar el sistema de red de iDRAC para obtener ayuda con la configuración inicial de la red del iDRAC.

Configuración de los valores de LAN de IPMI y de red

NOTA: Para poder realizar los pasos a continuación, se debe tener privilegio para **Configurar el iDRAC**.

NOTA: La mayoría de los servidores DHCP requieren un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este símbolo durante la negociación de DHCP. El iDRAC proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

1. Haga clic en **Sistema**→ **Acceso Remoto**→ **iDRAC**.

2. Haga clic en la ficha **Red/Seguridad** para abrir la página **Configuración de la red**.

   La tabla 5-1 y la tabla 5-2 describen la **Configuración de red** y la **Configuración de LAN de IPMI** en la página **Red**.

3. Cuando haya terminado de introducir los valores necesarios, haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-3.

Tabla 5-1. Configuración de red

Valor	Descripción
Activar NIC	Cuando se selecciona, indica que el NIC está activado y habilita los controles restantes en este grupo. Cuando un NIC está desactivado, toda la comunicación hacia el iDRAC y que provenga del mismo a través de la red está bloqueada. El valor predeterminado es **apagado**.
Dirección de control de acceso al medio (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. La dirección MAC no se puede cambiar.
Usar DHCP (Para la dirección IP de la tarjeta de interfaz de red)	Pide al iDRAC que obtenga una dirección IP para el NIC del servidor de Protocolo de configuración dinámica de host (DHCP). Asimismo, desactiva los controles **Dirección IP estática**, **Máscara de subred estática** y **Puerta de enlace estática**. El valor predeterminado es **apagado**.
Dirección IP estática	Permite ingresar o editar una dirección IP estática para el NIC del iDRAC. Para cambiar este valor, deseleccione la casilla de marcación **Usar DHCP (para dirección IP del NIC)**.
Máscara de subred estática	Permite ingresar o editar una máscara de subred para el NIC del iDRAC. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP (para la dirección IP del NIC)**.

Puerta de enlace estática	Permite ingresar o editar una puerta de enlace estática para el NIC del iDRAC. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP (para la dirección IP del NIC)**.
Usar DHCP para obtener direcciones de servidor DNS	Habilite el DHCP para obtener direcciones del servidor DNS por medio de la selección de la casilla **Use el DHCP para obtener direcciones de servidor DNS**. Cuando no se usa DHCP para obtener las direcciones del servidor DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**. El valor predeterminado es **apagado**. **NOTA:** Cuando la casilla **Use el DHCP para obtener direcciones de servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**.
Servidor DNS preferido estático	Permite al usuario ingresar o editar una dirección IP estática para el servidor DNS preferido. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP para obtener direcciones de servidor DNS**.
Servidor DNS alternativo estático	Usa la dirección IP del servidor DNS secundario cuando la opción **Usar DHCP para obtener direcciones de servidor DNS no está seleccionada**. Introduzca una dirección IP 0.0.0.0 si no hay ningún servidor DNS alternativo.
Registrar el iDRAC en DNS	Registra el nombre del iDRAC en el servidor DNS. El valor predeterminado es **Desactivado**.
Nombre DNS del iDRAC	Muestra el nombre del iDRAC únicamente cuando la opción **Registrar el iDRAC en DNS** está seleccionada. El nombre predeterminado es idrac-*etiqueta_de_servicio*, donde *etiqueta_de_servicio* es el número de la etiqueta de servicio del servidor Dell. Por ejemplo: idrac-00002.
Usar DHCP para el nombre del dominio de DNS	Usa el nombre de dominio DNS predeterminado. Cuando la casilla no está seleccionada y la opción **Registrar el iDRAC en DNS** está seleccionada, usted puede modificar el nombre de dominio DNS en el campo **Nombre de dominio DNS**. El valor predeterminado es **Desactivado**. **NOTA:** Para seleccionar la casilla **Usar DHCP para el nombre del dominio DNS**, seleccione también la casilla **Usar DHCP (para la dirección IP de NIC)**.
Nombre del dominio DNS	El **nombre de dominio DNS** predeterminado está en blanco. Cuando la casilla **Usar DHCP para el nombre del dominio DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.
Cadena de comunidad	Contiene la cadena de comunidad a usar en las capturas de alertas de **Protocolo simple de administración de red (SNMP)** enviadas desde el iDRAC. Las capturas de alertas SNMP son transmitidas por el iDRAC cuando ocurre un suceso de plataforma. El valor predeterminado es **public**.
Dirección del servidor SMTP	La dirección IP del servidor **SMTP (Protocolo simple de transferencia de correo)** con el que el iDRAC se comunica para enviar alertas por correo electrónico cuando ocurre un suceso de plataforma. El valor predeterminado es **127.0.0.1**.

Tabla 5-2. Configuración de la LAN IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando está seleccionado, indica que el canal LAN de IPMI está activado. El valor predeterminado es **apagado**.
Límite del nivel de privilegios del canal	Configura el nivel máximo de privilegio del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: **Administrador**, **Operador** o **Usuario**. El valor predeterminado es **Administrador**.
Clave de cifrado	Configura la clave de cifrado: de 0 a 20 caracteres hexadecimales (no se permiten espacios). De manera predeterminada está en blanco.

Tabla 5-3. Botones de la página de configuración de la red

Botón	Descripción
Configuración avanzada	Abre la página **Seguridad de la red**, permitiendo al usuario ingresar atributos del rango de IP y de bloqueo de IP.
Imprimir	Imprime los valores de la **Configuración de red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de red**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la página de configuración de la red. **NOTA:** Si se hacen cambios en la configuración de la dirección IP del NIC se cerrarán todas las sesiones de usuario y los usuarios tendrán que volver a conectarse a la interfaz web del iDRAC con la configuración actualizada de la dirección IP. Todos los demás cambios requerirán que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración de la filtración de IP y el bloqueo de IP

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

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y luego haga clic en la ficha **Red/Seguridad** para abrir la página **Configuración de la red**.
2. Haga clic en **Configuración avanzada** para configurar los valores de seguridad de la red.

La tabla 5-4 describe los valores de la página **Seguridad de la red**.

3. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-5.

Tabla 5-4. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango de IP, que define un rango de direcciones IP que puede acceder al iDRAC. El valor predeterminado es **apagado**.
Dirección del rango de IP	Determina la dirección de subred de IP aceptable. El valor predeterminado es **192.168.1.0**.
Máscara de subred del rango de IP	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. 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 **apagado**.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección. El valor predeterminado es **10**.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. El valor predeterminado es **3600.**

Tabla 5-5. Botones de la página de seguridad de la red

Botón	Descripción
Imprimir	Imprime los valores de la **Seguridad de la red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Seguridad de la red**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la página **Seguridad de la red**.
Volver a la página de red	Regresa a la página **Red**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma ofrece un mecanismo para configurar el iDRAC 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 5-6.

Tabla 5-6. Los sucesos de plataforma que se pueden filtrar

Índice	Suceso de plataforma
1	Declaración de advertencia de la batería
2	Declaración crítica de la batería
3	Declaración crítica de voltaje discreto
4	Declaración de advertencia de temperatura
5	Declaración crítica de temperatura
6	Redundancia degradada
7	Redundancia perdida
8	Declaración de advertencia del procesador
9	Declaración crítica del procesador
10	Declaración de ausencia del procesador
11	Declaración crítica de registro de sucesos
12	Declaración crítica de vigilancia

.

Cuando se presenta un suceso de plataforma (por ejemplo, la falla de una declaración de advertencia de la batería), se genera un suceso de sistema y se registra en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) que está activado y usted ha configurado el filtro para generar una alerta (PET o correo electrónico), se enviará una alerta por correo electrónico o captura de suceso de plataforma 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 ejecutará.

Configuración de los filtros de sucesos de plataforma (PEF)

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

1. Inicie sesión en la interfaz web del iDRAC. Consulte el apartado Acceso a la interfaz web.
2. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.
3. En la página de Sucesos de plataforma, active **Generación de alerta** para un suceso haciendo clic en la casilla **Generar alerta** que corresponda a ese suceso.

NOTA: Puede activar o desactivar la generación de alertas para todos los sucesos si hace clic en la casilla junto al encabezado de la columna Generar alerta.

4. Haga clic en el botón de radio debajo de la acción que desea activar para cada suceso. Sólo se puede configurar una acción para cada suceso.
5. Haga clic en **Aplicar**.

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

Configuración de capturas de suceso de plataforma (PET)

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

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte el apartado Acceso a la interfaz web.
2. Compruebe que siguió los procedimientos descritos en Configuración de los filtros de sucesos de plataforma (PEF).
3. Configure la dirección IP de destino de la PET:
   a. Haga clic en la casilla **Activar** junto al **Número de destino** que desea activar.
   b. Introduzca una dirección IP en el cuadro **Dirección IP de destino**.

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

   c. Haga clic en **Aplicar**.

   NOTA: Para tener éxito en el envío de una captura, configure el valor de la **Cadena de comunidad** en la página **Configuración de la red**. El valor de la **Cadena de comunidad** indica la cadena de comunidad que se va a usar en una captura de alertas de Protocolo simple de administración de red (SNMP) enviada desde el iDRAC. Las capturas de alertas SNMP son transmitidas por el iDRAC cuando ocurre un suceso de plataforma. El valor predeterminado de la **Cadena de comunidad** es **Public**.

   d. Haga clic en **Enviar** para probar la alerta configurada (si lo desea).
   e. Repita los pasos de la "a" a la "d" para los números de destino restantes.

Configuración de alertas por correo electrónico

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido.
2. Compruebe que siguió los procedimientos descritos en Configuración de los filtros de sucesos de plataforma (PEF).
3. Configure los valores de la alerta de correo electrónico
   a. En la ficha **Administración de alertas**, haga clic en **Configuración de alertas por correo electrónico**.
4. Configure el destino de la alerta por correo electrónico.
   a. En la columna **Número de alerta por correo electrónico**, haga clic en un número de destino. Hay cuatro destinos posibles para recibir alertas.
   b. Compruebe que la casilla **Activado** esté seleccionada.
   c. En el campo **Dirección de correo electrónico de destino**, escriba una dirección válida de correo electrónico.
   d. Haga clic en **Aplicar**.

NOTA: Para enviar correctamente un correo electrónico de prueba, la **Dirección del servidor SMTP** debe estar configurada en la página **Configuración de la red**. La dirección IP del **Servidor SMTP** se comunica con el iDRAC para enviar alertas por correo electrónico cuando ocurra un suceso de plataforma.

e. Haga clic en **Enviar** para probar la alerta por correo electrónico configurada (si lo desea).

f. Repita del paso a al paso e para las configuraciones restantes de alertas de correo electrónico.

Configuración de IPMI

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

2. Configure la IPMI en la LAN.

   a. Haga clic en **Sistema**→ **Acceso remoto**→ iDRAC, luego haga clic en **Red/Seguridad**.

   b. En la página **Configuración de la red** en **Configuración de la LAN de IPMI**, seleccione **Activar IPMI en la LAN**.

   c. Actualice los privilegios del canal de LAN de IPMI, si es necesario:

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

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

   d. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

NOTA: La IPMI de iDRAC es compatible con el protocolo RMCP+.

NOTA: La clave de cifrado debe constar de un número par de caracteres hexadecimales con un máximo de 20 caracteres.

En **Configuración de la LAN IPMI** en el campo **Clave de cifrado**, escriba la clave de cifrado.

   e. Haga clic en **Aplicar**.

3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

   a. Haga clic en **Sistema**→ **Acceso Remoto**→ **iDRAC**.

   b. Haga clic en la ficha **Seguridad de la red** y después haga clic en **Comunicación en serie en la LAN**.

   c. En la página **Configuración de la comunicación en serie en la LAN**, haga clic en la casilla **Activar comunicación en serie en la LAN** para habilitar la 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 que la velocidad en baudios de SOL sea idéntica a la velocidad en baudios del servidor administrado.

Haga clic en el menú desplegable **Velocidad en baudios** para seleccionar una velocidad de datos de 19,2 kbps, 57,6 kbps o 115,2 kbps.

   e. Haga clic en **Aplicar**.

Cómo agregar y configurar usuarios de iDRAC

Para administrar el sistema con el iDRAC y mantener la seguridad del sistema, cree usuarios únicos con permisos administrativos específicos (o con *autoridad basada en funciones*).

Para agregar y configurar los usuarios de iDRAC, realice los pasos a continuación:

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

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Red/Seguridad**.

2. Abra la página **Usuarios** para configurar usuarios.

   La página **Usuarios** muestra la **Identificación de usuario**, **Estado**, **Nombre de usuario**, **Privilegios de LAN de IPMI**, **Privilegios del iDRAC** y **Comunicación en serie en la LAN** de cada usuario.

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

3. En la columna **Id. de usuario**, haga clic en un número de identificación de usuario.

4. En la página **Configuración de usuario**, configure las propiedades y los privilegios de usuario.

   La tabla 5-7 describe los valores **Generales** de configuración de un nombre de usuario y contraseña del iDRAC.

   La tabla 5-8 describe los **Privilegios de la LAN de IPMI** para configurar los privilegios de LAN del usuario.

   La tabla 5-9 describe los permisos del **Grupo de usuarios** para la configuración de los **Privilegios de LAN de IPMI** y de los **Privilegios de usuario del iDRAC**.

   La tabla 5-10 describe los permisos de **Grupo de iDRAC**. Si agrega un **Privilegio de usuario de iDRAC** al grupo de **Administrador**, **Usuario avanzado** o **Usuario invitado**, el **Grupo de iDRAC** cambiará a grupo **Personalizado**.

5. Cuando termine, haga clic en **Aplicar**.

6. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-11.

Tabla 5-7. Propiedades generales

Propiedad	Descripción
Identificación de usuario	Contiene uno de los 16 números preconfigurados de identificación de usuario. Este campo no se puede editar.
Activar el usuario	Cuando está seleccionado, indica que el acceso del usuario al iDRAC está activado. Cuando no está seleccionado, el acceso de usuario está desactivado.
Nombre de usuario	Especifica un nombre de usuario de iDRAC de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único. **NOTA:** Los nombres de usuario de iDRAC no pueden incluir los caracteres de **/** (diagonal) ni **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Cambiar contraseña	Activa los campos **Nueva contraseña** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Activa la edición de la contraseña del usuario del iDRAC. Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán.
Confirmar nueva contraseña	Vuelva a escribir la contraseña del usuario del iDRAC para confirmarla.

Tabla 5-8. Privilegios del usuario en la LAN de IPMI

Propiedad	Descripción
Privilegio máximo permitido de usuario de LAN	Especifica el privilegio máximo del usuario en el canal de LAN de IPMI como uno de los siguientes grupos de usuario: **Ninguno**, **Administrador**, **Operador** o **Usuario**.
Activar comunicación en serie en la LAN.	Permite al usuario usar la comunicación en serie en la LAN de IPMI. Cuando se selecciona, este privilegio se activa.

Tabla 5-9. Privilegios del usuario del iDRAC

Propiedad	Descripción
Grupo de iDRAC	Especifica el privilegio máximo del usuario de iDRAC como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Personalizado** o **Ninguno**. Consulte la tabla 5-10 para ver los permisos del **Grupo de iDRAC**.
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros de iDRAC.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a redirección de consola	Activa la capacidad del usuario de ejecutar redirección de consola.
Acceder a los medios virtuales	Activa la capacidad del usuario de ejecutar y usar los medios virtuales.
Probar alertas	Activa la capacidad del usuario de enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Activa la capacidad del usuario de ejecutar comandos de diagnóstico.

Tabla 5-10. Permisos de grupo del iDRAC

Grupo de usuarios	Permisos concedidos
Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.
Usuario avanzado	**Iniciar sesión en el iDRAC**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**
Usuario invitado	**Inicio de sesión en iDRAC**
Personalizado	Selecciona cualquier combinación de los permisos siguientes: **Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de acción del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**
Ninguno	Sin permisos asignados

Tabla 5-11. Botones de la página de configuración de usuario

Botón	Acción
Imprimir	Imprime los valores de la **Configuración de usuario** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de usuario**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la configuración de usuario.
Volver a la página de usuarios	Regresa a la **página de usuarios**.

Cómo asegurar las comunicaciones de iDRAC por medio de certificados SSL y digitales

Esta sección ofrece información sobre las funciones de seguridad de datos siguientes que vienen incorporadas en el iDRAC:

- Capa de conexión segura (SSL)
- Solicitud de firma de certificado (CSR)
- Cómo acceder al menú principal de SSL
- La generación de nuevo CSR
- Cómo cargar un certificado de servidor
- Cómo ver un certificado de servidor

Capa de conexión segura (SSL)

El iDRAC incluye un servidor web que está configurado para usar el protocolo de seguridad SSL -que es el estándar de la industria- para transferir datos cifrados a través de una red. Como está cimentado en la tecnología de cifrado de claves privada y pública, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autentificada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Se autentifique a sí mismo ante un cliente habilitado con SSL
- Permita que el cliente se autentifique a sí mismo ante el servidor
- Permita que ambos sistemas establezcan una conexión cifrada

El proceso de cifrado proporciona un alto nivel de protección de datos. El iDRAC emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está normalmente disponible para los exploradores de Internet en Norteamérica.

De manera predeterminada, el servidor web de iDRAC tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en la Internet, sustituya el certificado de SSL del servidor web con un certificado firmado por una autoridad reconocida de certificados. Para iniciar el proceso de obtención de un certificado firmado, se puede usar la interfaz web del iDRAC para generar una solicitud de firma de certificado (CSR) con la información de la empresa. Usted podrá enviar entonces la CSR generada a una autoridad de certificados como VeriSign o Thawte.

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (CA) para obtener un certificado de servidor seguro. Los certificados de servidor seguro hacen que los clientes del servidor confíen en la identidad del servidor al que se conectan y que negocien una sesión cifrada con el servidor.

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

Después de que la autoridad de certificados apruebe la CSR y envíe el certificado, cargue el certificado en el firmware del iDRAC. La información de la CSR almacenada en el firmware del iDRAC debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Red/Seguridad**.
2. Haga clic en **SSL** para abrir la página **Menú principal de SSL**.

Use la página **Menú principal de SSL** para generar una CSR para enviarla a una autoridad de certificados. La información de la CSR se almacena en el firmware del iDRAC.

La tabla 5-12 describe las opciones disponibles al momento de generar una CSR.

La tabla 5-13 describe los botones disponibles en la página **Menú principal de SSL**.

Tabla 5-12. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	Seleccione la opción y haga clic en **Siguiente** para abrir la página **Generar solicitud de firma de certificado (CSR)**. **NOTA:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la CA acepte la CSR, la CSR?que está en el firmware debe coincidir con el certificado que la CA devuelve.
Cargar certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la página **Carga del certificado** y cargar el certificado que recibió de la autoridad de certificados. **NOTA:** El iDRAC sólo acepta certificados codificados con X509, base 64. No acepta certificados codificados DER.
Ver el certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la página **Ver certificado del servidor** y ver un certificado de servidor existente.

Tabla 5-13. Botones del menú principal de SSL

Botón	Descripción
Imprimir	Imprime los valores del **Menú principal de SSL** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Menú principal de SSL**.
Next	Procesa la información de la página **Menú principal de SSL** y continúa al siguiente paso.

Generación de una nueva solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. La CSR en el firmware debe coincidir con el certificado que recibió de la autoridad de certificados. De lo contrario, el iDRAC no aceptará el certificado.

1. En la página **Menú principal de SSL**, seleccione **Generar una nueva 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 5-14 describe las opciones de la página **Generar solicitud de firma de certificado (CSR)**.
3. Haga clic en **Generar** para crear la CSR.
4. Haga clic en **Descargar** para guardar el archivo de la CSR en el equipo local.
5. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-15.

Tabla 5-14. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **www.empresaxyz.com**). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Tecnología informática). Sólo son válidos

organizacional	los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Monterrey). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo u otro carácter.
Nombre del estado:	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Nuevo León). Sólo son válidos los caracteres alfanuméricos y los espacios. No use abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Escriba la dirección de correo electrónico de la empresa o cualquier dirección de correo electrónico asociada con la CSR. Este campo es opcional.

Tabla 5-15. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime los valores de **Generar solicitud de firma de certificado** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Generar solicitud de firma de certificado**.
Generar	Genera una CSR y luego pide al usuario que lo guarde en un directorio específico.
Descargar	Descarga el certificado en el equipo local.
Volver al menú principal de SSL	Regresa al usuario a la página **Menú principal de SSL**.

Carga de un certificado de servidor

1. En la página **Menú principal de SSL**, seleccione **Cargar certificado de servidor** y haga clic en **Siguiente**.

   Aparecerá la página **Carga de certificado**.

2. En el campo **Ruta de acceso del archivo**, escriba la ruta de acceso al certificado o haga clic en **Examinar** para desplazarse hacia el archivo del certificado.

NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

3. Haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-16.

Tabla 5-16. Botones de la página de carga de certificados

Botón	Descripción
Imprimir	Imprime los valores que aparecen en la página **Carga del certificado**.
Actualizar	Vuelve a cargar la página **Carga del certificado**.
Aplicar	Aplica el certificado al firmware del iDRAC.
Volver al menú principal de SSL	Regresa al usuario a la página **Menú principal de SSL**.

Cómo ver un certificado de servidor

1. En la página **Menú principal de SSL**, seleccione **Ver certificado del servidor** y haga clic en **Siguiente**.

   La tabla 5-17 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-18.

Tabla 5-17. Información de certificados

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

Tabla 5-18. Botones de página de visualización de certificados del servidor

Botón	Descripción
Imprimir	Imprime los valores de **Ver certificado del servidor** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Ver certificado del servidor**.
Volver al menú principal de SSL	Regresa a la página **Menú principal de SSL**.

Configuración y administración de certificados de Active Directory

NOTA: Debe tener permiso para **Configurar el iDRAC** a fin de configurar Active Directory y cargar, descargar y ver un certificado de Active Directory.

NOTA: Para obtener más información acerca de la configuración de Active Directory y sobre cómo configurar Active Directory con el esquema estándar o un esquema ampliado, consulte Uso de iDRAC con Microsoft Active Directory.

Para acceder al **Menú principal de Active Directory**:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC,** luego haga clic en la ficha **Red / Seguridad**.
2. Haga clic en **Active Directory** para abrir la página **Menú principal de Active Directory**.

   La tabla 5-19 muestra una lista de las opciones de la página **Menú principal de Active Directory**.
3. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 5- 20.

Tabla 5-19. Opciones de la página de menú principal de Active Directory

Campo	Descripción
Configurar Active Directory	Configura los valores **Nombre de dominio raíz**, **Tiempo de espera de autentificación de Active Directory**, **Selección del esquema de Active Directory**, **Nombre del iDRAC**, **Nombre de dominio del iDRAC**, **Grupos de funciones**, **Nombre de grupo** y **Dominio del grupo de Active Directory**.
Cargar un certificado de CA de Active Directory	Carga un certificado de Active Directory al iDRAC.
Descargar certificado del servidor de iDRAC	El **Administrador de descargas de Windows** descarga un certificado de servidor de iDRAC al sistema.
Ver un certificado de CA de Active Directory	Muestra el certificado de Active Directory que ha sido cargado en el iDRAC.

Tabla 5-20. Botones de la página de menú principal de Active Directory

Botón	Definición
Imprimir	Imprime los valores del **Menú principal de Active Directory** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Menú principal de Active Directory**.
Next	Procesa la información de la página **Menú principal de Active Directory** y continúa al siguiente paso.

Configuración de Active Directory, (esquema estándar y esquema ampliado)

1. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.
2. En la página **Configuración de Active Directory**, introduzca los valores de Active Directory.

   La tabla 5-21 describe los valores de la página **Configuración y administración de Active Directory**.
3. Haga clic en **Aplicar** para guardar la configuración.
4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-22.
5. Para configurar los grupos de funciones para el esquema estándar de Active Directory, haga clic en el grupo de funciones individual (1 a 5). Consulte el apartado tabla 5-23 y el apartado tabla 5-24.

NOTA: Para guardar los valores de la página **Configuración de Active Directory**, haga clic en **Aplicar** antes de proceder con la página **Grupo de funciones personalizado**.

Tabla 5-21. Valores de la página de configuración de Active Directory

Valor	Descripción
Activar Active Directory	Cuando está seleccionado, activa Active Directory. El valor predeterminado es **desactivado**.
Nombre del dominio RAÍZ	El nombre de dominio RAÍZ de Active Directory. De manera predeterminada está en blanco. El nombre debe ser un nombre de dominio válido que consista de *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios en blanco entre ellos y *y* es un tipo de dominio válido como com, edu, gov, int, mil, red u org. De manera predeterminada está en blanco.
Tiempo de espera	El tiempo en segundos para completar consultas de Active Directory. El valor mínimo es igual o mayor que 15 segundos. El valor predeterminado es **120**.
Usar el esquema estándar	Usa el esquema estándar con Active Directory.
Usar el esquema ampliado	Usa el esquema ampliado con Active Directory.
Nombre del iDRAC	El nombre que identifica de manera exclusiva el iDRAC en Active Directory. De manera predeterminada está en blanco. El nombre debe ser una cadena de 1 a 254 caracteres ASCII, sin espacios entre ellos.
Nombre del dominio de iDRAC	El nombre DNS del dominio donde reside el objeto iDRAC de Active Directory. De manera predeterminada está en blanco. El nombre debe ser un nombre de dominio válido que consista de *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios en blanco entre ellos y *y* es un tipo de dominio válido como com, edu, gov, int, mil, red u org.
Grupos de funciones	La lista de grupos de funciones que está relacionada con el iDRAC. Para cambiar la configuración de un grupo de función, haga clic en el número del grupo de funciones, en la lista de grupos de funciones.
Nombre de grupo	El nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC. De manera predeterminada está en blanco.
Dominio de grupo	El tipo de dominio en donde reside el grupo de funciones.

Tabla 5-22. Botones de la página de configuración de Active Directory

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de Active Directory** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de Active Directory**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la página **Configuración de Active Directory**.
Volver al menú principal de Active Directory	Regresa a la página **Menú principal de Active Directory**.

Tabla 5-23. Privilegios del grupo de funciones

Valor	Descripción
Nivel de privilegio del grupo de funciones	Especifica el privilegio máximo del usuario de iDRAC como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Ninguno** o **Personalizado**. Consulte la tabla 5-24 para ver los permisos del **Grupo de funciones**.
Inicio de sesión en iDRAC	Permite que el grupo inicie sesión en el iDRAC.
Configurar iDRAC	Da permiso al grupo para configurar el iDRAC.
Configurar usuarios	Da permiso al grupo para configurar usuarios.
Borrar registros	Da permiso al grupo para borrar registros.
Ejecutar comandos de control del servidor	Da permiso al grupo para ejecutar comandos de control del servidor.
Acceder a redirección de consola	Permite que el grupo tenga acceso a la redirección de consola.
Acceder a los medios virtuales	Permite que el grupo tenga acceso a los medios virtuales.
Probar alertas	Permite al grupo enviar alertas de prueba (mensajes de correo electrónico y capturas de sucesos de plataforma) a un usuario específico.
Ejecutar comandos de diagnóstico	Da permiso al grupo para ejecutar comandos de diagnóstico.

Tabla 5-24. Permisos del grupo de funciones

Propiedad	Descripción
Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.

Usuario avanzado	**Iniciar sesión en el iDRAC**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**
Usuario invitado	**Inicio de sesión en iDRAC**
Personalizado	Selecciona cualquier combinación de los permisos siguientes: **Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de acción del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**
Ninguno	Sin permisos asignados

Cómo cargar un certificado de CA de Active Directory

1. En la página **Menú principal de Active Directory**, seleccione **Cargar certificado de CA de Active Directory** y haga clic en **Siguiente**.
2. En la página **Carga del certificado**, escriba la ruta de acceso del certificado en el campo **Ruta de acceso del archivo** o haga clic en **Examinar** para desplazarse al archivo de 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 al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

Asegúrese de que los certificados SSL del controlador de dominio estén firmados por la misma autoridad de certificados y que el certificado esté disponible en la estación de administración que esté accediendo al iDRAC.

3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-25.

Tabla 5-25. Botones de la página de carga de certificados

Botón	Descripción
Imprimir	Imprime los valores de **Carga del certificado** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Carga del certificado**.
Aplicar	Aplica el certificado al firmware del iDRAC.
Volver al menú principal de Active Directory	Regresa a la página **Menú principal de Active Directory**.

Descarga de un certificado de servidor del iDRAC

1. En la página **Menú principal de Active Directory**, seleccione **Descargar certificado de servidor de iDRAC** y haga clic en **Siguiente**.
2. Guarde el archivo en un directorio del sistema.
3. En la ventana **Descarga completa**, haga clic en **Cerrar**.

Cómo ver un certificado de CA de Active Directory

Use la página **Menú principal de Active Directory** para ver un certificado de servidor de CA de iDRAC.

1. En la página **Menú principal de Active Directory**, seleccione **Ver certificado de CA de Active Directory** y haga clic en **Siguiente**.

   La tabla 5-26 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-27.

Tabla 5-26. Información del certificado de CA de Active Directory

Campo	Descripción
Número de serie	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.
Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Tabla 5-27. Botones de la página Ver certificado de CA de Active Directory

Botón	Descripción
Imprimir	Imprime los **valores del certificado de CA de Active Directory que aparecen en la pantalla**.
Actualizar	Vuelve a cargar la página **Certificado de CA de Active Directory.**
Volver al menú principal de Active Directory	Regresa al usuario a la página **Menú principal de Active Directory**.

Activación o desactivación del acceso a la configuración local

NOTA: La configuración predeterminada para el acceso a la configuración local es **Activado**.

Activación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. En **Configuración local**, haga clic para deseleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC local** para activar el acceso.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente.

Desactivación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. En **Configuración local**, haga clic para deseleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC local** para activar el acceso.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente.

Configuración de la comunicación en serie en la LAN

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. Haga clic en **Comunicación en serie en la LAN** para abrir la página **Configuración de la comunicación en serie en la LAN**.

   La tabla 5-28 contiene información sobre los valores de la página **Configuración de la comunicación en serie en la LAN**.
3. Haga clic en **Aplicar**.
4. Defina la configuración avanzada, si es necesario. De lo contrario, haga clic en el botón correspondiente para continuar (ver tabla 5-29)

   Para definir la configuración avanzada, realice los pasos siguientes:

   a. Haga clic en **Configuración avanzada**.

   b. En la página **Configuración avanzada de la comunicación en serie en la LAN**, defina la configuración avanzada según sea necesario (ver tabla 5-30).

   c. Haga clic en **Aplicar**.

   d. De lo contrario, haga clic en el botón correspondiente para continuar (ver tabla 5-31)

Tabla 5-28. Valores de la página de configuración de la comunicación en serie en la LAN

Valor	Descripción

Activar comunicación en serie en la LAN.	Cuando está seleccionada, la casilla indica que la comunicación en serie en la LAN está activada.
Velocidad en baudios	Indica la velocidad de los datos. Seleccione una velocidad de datos de **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.

Tabla 5-29. Botones de la página de configuración de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de la comunicación en serie en la LAN** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de la comunicación en serie en la LAN.**
Configuración avanzada	Abre la página **Configuración avanzada de la comunicación en serie en la LAN**.
Aplicar	Aplica los nuevos valores que se asignen mientras se consulta la **Configuración de la comunicación en serie en la LAN**.

Tabla 5-30. Valores de la página de configuración avanzada de la comunicación en serie en la LAN

Valor	Descripción
Intervalo de acumulación de caracteres	La cantidad de tiempo que el iDRAC esperará antes de transmitir un paquete parcial de datos de caracteres SOL. El tiempo se mide en segundos.
Umbral de envío de caracteres	El iDRAC enviará un paquete de datos de caracteres SOL tan pronto como se acepte al menos este número de caracteres. El umbral se mide en caracteres.

Tabla 5-31. Botones de la página de configuración avanzada de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración avanzada de la comunicación en serie en la LAN** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración avanzada de la comunicación en serie en la LAN**.
Aplicar	Guarda cualquier configuración nueva que asigne mientras esté en la página **Configuración avanzada de la comunicación en serie en la LAN**.
Volver a la página de configuración de la comunicación en serie en la LAN	Regresa al usuario a la página **Configuración de la comunicación en serie en la LAN**.

Configuración de los servicios de iDRAC

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

NOTA: Cuando se aplican cambios en los servicios, los cambios surten efecto inmediatamente. Las conexiones existentes pueden ser terminadas sin advertencia.

NOTA: Existe un problema conocido con el cliente Telnet suministrado con Microsoft Windows y la comunicación con una BMU. Use otro cliente Telnet como HyperTerminal o PuTTY.

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Red/Seguridad**.
2. Haga clic en **Servicios** para abrir la página de configuración **Servicios**.
3. Configure los servicios siguientes según sea necesario:
   - Servidor web: consulte la tabla 5-32 para ver la configuración del servidor web
   - SSH: consulte la tabla 5-33 para ver la configuración de SSH
   - Telnet: consulte la tabla 5-34 para ver la configuración de Telnet
   - Agente de recuperación automatizada del sistema: consulte la tabla 5-35 para ver la configuración del agente de recuperación automatizada del sistema
4. Haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 5-36.

Tabla 5-32. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor web del iDRAC. Cuando está seleccionada, la casilla indica que el servidor web está activado. El valor predeterminado es **activado**.

Nº. máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Este campo no se puede editar. Pueden existir cuatro sesiones simultáneas.
Sesiones actuales	El número de sesiones actuales en el sistema, menor o igual al **Nº. 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 en el valor de tiempo de espera surtirán efecto inmediatamente y restablecerán el servidor web. El rango del tiempo de espera es de 60 a 1920. El valor predeterminado es de **300** segundos.
Número de puerto de HTTP	El puerto en el que el iDRAC espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto de HTTPS	El puerto en el que el iDRAC espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 5-33. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando está seleccionada, la casilla indica que SSH está activado.
Nº. máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Sólo se admite una sesión.
Sesiones activas	El número de sesiones actuales en el sistema.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango del tiempo de espera es de 60 a 1920. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC espera una conexión SSH. El valor predeterminado es **22**.

Tabla 5-34. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado.
Nº. máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Sólo se admite una sesión.
Sesiones activas	El número de sesiones actuales en el sistema.
Tiempo de espera	El tiempo de espera en inactividad del telnet, en segundos. El rango del tiempo de espera es de 60 a 1920. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **0**.
Número de puerto	El puerto en el que el iDRAC espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 5-35. Configuración del agente de recuperación automatizada del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automatizada del sistema.

Tabla 5-36. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

Actualización del firmware del iDRAC

AVISO: Si el firmware del iDRAC se daña, como puede suceder cuando el progreso de actualización del firmware del iDRAC se interrumpe antes de terminar, usted puede recuperar el iDRAC por medio del CMC. Consulte su *Guía del usuario del firmware del CMC* para obtener instrucciones.

NOTA: De manera predeterminada, la actualización del firmware retendrá la configuración actual del iDRAC. Durante el proceso de actualización, usted tiene la opción de restablecer los valores predeterminados de fábrica para la configuración del iDRAC. Si usted establece la configuración predeterminada de fábrica, el acceso a la red externa se desactivará cuando la actualización termine. Usted debe activar y configurar la red por medio de la utilidad de configuración del iDRAC o de la interfaz web del CMC.

1. Inicie la interfaz web del iDRAC.

2. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Actualizar**.

   NOTA: Para actualizar el firmware, el iDRAC debe estar en el modo de actualización. Cuando se encuentre en este modo, el iDRAC se restablecerá automáticamente, aun cuando usted cancele el proceso de actualización.

3. En la página **Actualización del firmware**, haga clic en **Siguiente** para iniciar el proceso de actualización.

4. En la ventana **Actualización del firmware: Cargar (página 1 de 4)**, haga clic en **Examinar** o escriba la ruta de acceso de la imagen del firmware que descargó.

   Por ejemplo:

   `C:\Updates\V1.0\<nombre_de_imagen>`.

   El nombre predeterminado de la imagen del firmware es **firmimg.imc**.

5. Haga clic en **Siguiente**.

   - El archivo se cargará en el iDRAC. This may take several minutes to complete.

     O bien:

   - Puede hacer clic en **Cancelar** en este momento si lo que desea es terminar el proceso de actualización de firmware. Al hacer clic en **Cancelar**, el iDRAC se restablecerá al modo de operación normal.

- En la ventana **Actualización del firmware: Validación (página 2 de 4)**, verá los resultados de la validación hecha en el archivo de imagen que cargó.

  - Cuando el archivo de imagen se cargue exitosamente y pase todas las revisiones de verificación, aparecerá un mensaje indicando que la imagen del firmware ha sido verificada.

    O bien:

  - Cuando la imagen no se cargue correctamente o cuando no pase las revisiones de verificación, la actualización del firmware regresará a la ventana **Actualización del firmware: Cargar (página 1 de 4)**. Puede intentar actualizar el iDRAC nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC al modo de operación normal.

NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada. Usted no podrá iniciar sesión en la interfaz web del iDRAC. Usted deberá reconfigurar los valores de la LAN por medio de la interfaz web del CMC o iKVM por medio de la utilidad de configuración del iDRAC durante la POST del BIOS.

7. De manera predeterminada, la casilla de marcación **Conservar configuración** está seleccionada, esto es para conservar los valores actuales en el iDRAC después de una actualización. Si no desea conservar los valores, deseleccione la casilla **Conservar configuración**.

8. Haga clic en **Comenzar la actualización** para iniciar el proceso de actualización. No interrumpa el proceso de actualización.

9. En la ventana **Actualización del firmware: Actualización (página 3 de 4)**, verá el estado de la actualización. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.

10. Una vez que la actualización del firmware concluya, aparecerá la ventana **Actualización del firmware: Resultados de la actualización (página 4 de 4)** y el iDRAC se restablecerá automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC usando una ventana nueva de explorador.

Recuperación del firmware del iDRAC por medio del CMC

Normalmente, el firmware del iDRAC se actualiza por medio de los servicios de iDRAC, por ejemplo, la interfaz web del iDRAC o los paquetes de actualización específicos del sistema operativos que descargó del **support.dell.com**.

Si el firmware del iDRAC se daña, como podría ocurrir si el progreso de actualización del firmware del iDRAC se interrumpe antes de terminar, usted puede usar la interfaz web del CMC para actualizar el firmware.

Si el CMC detecta el firmware dañado del iDRAC, el iDRAC aparecerá en la página **Componentes que se pueden actualizar** en la interfaz web del CMC.

NOTA: Consulte la *Guía del usuario del firmware del CMC* para obtener instrucciones sobre cómo usar la interfaz web del CMC.

Para actualizar el firmware del iDRAC, realice los pasos siguientes:

1. Descargue el firmware del iDRAC más reciente en el equipo de administración de la dirección **support.dell.com**.

2. Inicie la sesión en la interfaz basada en web de la CMC.

3. Haga clic en **Chasis en el árbol del sistema**.

4. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**. El servidor con el iDRAC que se puede recuperar se incluirá en la lista siempre se pueda recuperar a partir del CMC.

5. Haga clic en **servidor-*n***, donde ***n*** es el número de servidor cuyo iDRAC desea recuperar.
6. Haga clic en **Examinar**, para desplazarse a la imagen del firmware del iDRAC que descargó y haga clic en **Abrir**.
7. Haga clic en **Iniciar actualización del firmware**.

Después de que el archivo de la imagen del firmware ha sido cargado al CMC, el iDRAC se actualizará a sí mismo con la imagen.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de iDRAC con Microsoft Active Directory

Guía del usuario de Integrated Dell™ Remote Access Controller versión 1.2

Un servicio de directorio mantiene una base de datos común de toda la información necesaria para controlar usuarios, equipos, impresoras y otros dispositivos en una red. Si la empresa usa el software de servicio Microsoft® Active Directory®, usted puede configurarlo de manera que tenga acceso al iDRAC, lo que le permite agregar y controlar los privilegios de usuario de iDRAC de los usuarios existentes en el software Active Directory.

NOTA: El uso de Active Directory para reconocer a los usuarios del iDRAC se admite en los sistemas operativos Microsoft Windows® 2000 y Windows Server® 2003.

Usted puede usar Active Directory para definir el acceso de los usuarios al iDRAC por medio de una solución de esquema ampliado que emplea objetos de Active Directory definidos por Dell, o bien, una solución de esquema estándar que emplea únicamente objetos de grupo de Active Directory.

Ventajas y desventajas del esquema ampliado y del esquema estándar

Cuando se usa Active Directory para configurar el acceso al iDRAC, se debe elegir la solución de esquema ampliado o de esquema estándar.

Las ventajas de usar la solución de esquema ampliado son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Se tiene la máxima flexibilidad para configurar el acceso que tienen los usuarios a distintos iDRAC con distintos niveles de privilegio.

Las ventajas de usar la solución de esquema estándar son:

- No se requiere la ampliación del esquema porque el esquema estándar usa únicamente objetos de Active Directory.
- La configuración de Active Directory es sencilla.

Generalidades del esquema ampliado de Active Directory

Hay tres maneras de activar Active Directory con el esquema ampliado:

- Con la interfaz web iDRAC (ver Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web).
- Con la herramienta RACADM CLI (ver Configuración del iDRAC con Active Directory de esquema ampliado por medio de RACADM).
- Con la línea de comandos SM-CLP (ver Configuración del iDRAC con Active Directory de esquema ampliado y SM-CLP).

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden ampliar la base de datos de Active Directory al agregar sus propios atributos y clases únicos para solucionar necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los atributos y las clases a fin de admitir la autentificación y autorización de administración remota.

Cada atributo o clase que es se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de Identificadores de Objeto de Active Directory (OID) de modo que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para ampliar el esquema en Microsoft Active Directory, Dell recibió identificaciones de objeto únicas, extensiones de nombre únicas e identificaciones de atributos con vínculos únicos para los atributos y clases que agregamos al servicio de directorio, según se muestra en la tabla 6-1.

Tabla 6-1. Identificadores de objeto de Active Directory de Dell

Clase de servicio de Active Directory	Identificación de objeto de Active Directory
Extensión de Dell	dell
OID de base Dell	1.2.840.113556.1.8000.1280
Rango de LinkID del RAC	De 12070 a 12079

Descripción de las extensiones de esquema de RAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha ampliado el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos de RAC. Este modelo proporciona al administrador la máxima flexibilidad sobre las combinaciones diferentes de usuarios, privilegios de RAC y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción general de los objetos de Active Directory

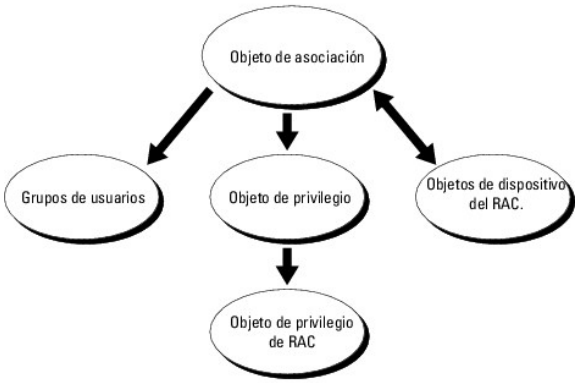
Para cada uno de los RAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de RAC. Puede crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios, grupos de usuarios u objetos de dispositivo de RAC sean necesarios. Los usuarios y objetos de dispositivo de RAC pueden ser miembros de cualquier dominio en la empresa.

Sin embargo, cada objeto de asociación puede ser vinculado (o, puede unir usuarios, grupos de usuarios u objetos de dispositivo de RAC) a sólo un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los RAC específicos.

El objeto del dispositivo del RAC es el eslabón al firmware de RAC para consultar a Active Directory para la autentificación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC 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. El administrador también deberá agregar el RAC por lo menos a un objeto de asociación para que los usuarios se puedan autentificar.

La figura 6-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

Figura 6-1. Configuración típica de los objetos de Active Directory



NOTA: El objeto de privilegio del RAC se aplica al DRAC 4 y al iDRAC.

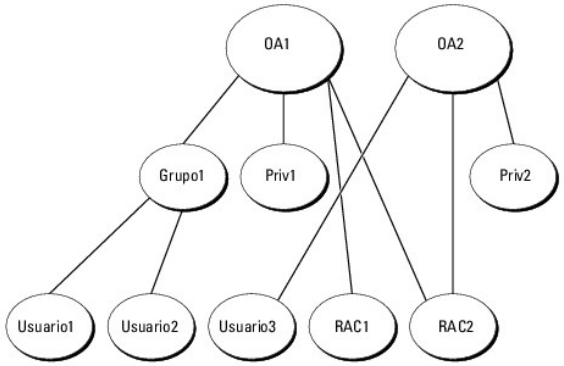
Usted puede crear tantos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de RAC para cada RAC (iDRAC) en la red que desea integrar con Active Directory para fines de autentificación y autorización con el RAC (iDRAC).

El objeto de asociación permite esta cantidad de usuarios y/o grupos así como objetos de dispositivo de RAC. Sin embargo, el objeto de asociación sólo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los "Usuarios" que tienen "Privilegios" en los RAC.

Usted puede configurar objetos de Active Directory en un solo dominio o en varios dominios. Por ejemplo, digamos que usted tiene dos iDRAC (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). Usted desea dar privilegios de administrador a usuario1 y usuario2 para los dos iDRAC y quiere dar privilegio de inicio de sesión a usuario3 para el RAC2. Figura 6-2 muestra cómo configurar los objetos de Active Directory en este caso.

Cuando se agregan grupos universales a partir de dominios independientes, se debe crear un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados creados por la utilidad Dell Schema Extender, son grupos locales de dominio y no funcionarán con grupos universales de otros dominios.

Figura 6-2. Configuración de objetos de Active Directory en un solo dominio



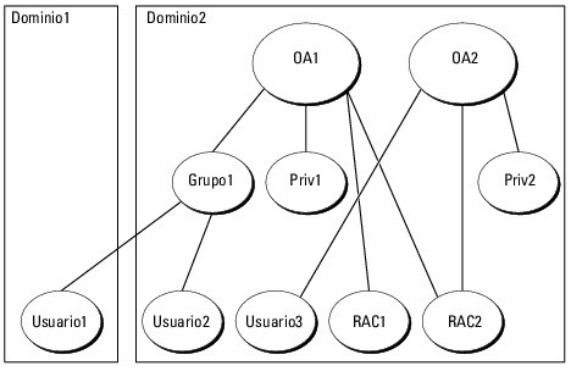
Para configurar los objetos para el escenario de un solo dominio, realice las siguientes tareas:

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC (RAC1 y RAC2) para representar los dos iDRAC.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
4. Agrupe al usuario1 y usuario2 en el Grupo1.
5. Agregue el Grupo1 como miembro en el objeto de asociación 1 (OA1), Priv1 como objeto de privilegio en OA1, y RAC1 y RAC2 como dispositivos de RAC en OA1.
6. Agregue el usuario3 como miembro en el objeto de asociación 2 (OA2), Priv2 como objeto de privilegio en OA2, y RAC2 como dispositivo de RAC en OA2.

Consulte Cómo agregar usuarios y privilegios de iDRAC a Active Directory para obtener instrucciones detalladas.

La figura 6-3 muestra un ejemplo de los objetos de Active Directory en varios dominios. En este escenario, usted tiene dos iDRAC (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). El usuario1 está en el Dominio1; el usuario2 y el usuario 3 están en el Dominio2. En este escenario, configure el usuario1 y el usuario2 con privilegios de administrador en los dos iDRAC y configure el usuario3 con privilegios de inicio de sesión para el RAC2.

Figura 6-3. Configuración de objetos de Active Directory en múltiples dominios



Para configurar los objetos en el caso de varios dominios, realice las siguientes tareas:

1. Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2. Cree dos objetos de asociación, OA1 (con ámbito universal) y OA2, en cualquier dominio.

   La figura 6-3 muestra los objetos en el Dominio2.
3. Cree dos objetos de dispositivo de RAC (RAC1 y RAC2) para representar los dos iDRAC.
4. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
5. Agrupe al usuario1 y usuario2 en el Grupo1. El ámbito de grupo del Grupo1 debe ser Universal.
6. Agregue el Grupo1 como miembro en el objeto de asociación 1 (OA1), Priv1 como objeto de privilegio en OA1, y RAC1 y RAC2 como dispositivos de RAC

en OA1.

7. Agregue el usuario3 como miembro en el objeto de asociación 2 (OA2), Priv2 como objeto de privilegio en OA2, y RAC2 como dispositivo de RAC en OA2.

Configuración de Active Directory de esquema ampliado para acceder al iDRAC

Antes de usar el Active Directory para acceder al iDRAC, debe configurar el software Active Directory y el iDRAC llevando a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (consulte Extensión del esquema de Active Directory).
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory).
3. Agregue usuarios de iDRAC y sus privilegios a Active Directory (consulte Cómo agregar usuarios y privilegios de iDRAC a Active Directory).
4. Active SSL en cada uno de los controladores de dominio (consulte Activación de SSL en un controlador de dominio).
5. Configure las propiedades de Active Directory de iDRAC por medio de la interfaz web del iDRAC o la RACADM (consulte Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web o Configuración del iDRAC con Active Directory de esquema ampliado por medio de RACADM).

Extensión del esquema de Active Directory

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

Puede ampliar su esquema usando una de las siguientes alternativas:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos LDIF

Si usa 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 CD *Dell Systems Management Consoles* en los siguientes directorios respectivamente:

- *Unidad de CD*:\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files
- *Unidad de CD*:\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender

Para usar los archivos LDIF, consulte las instrucciones en el archivo readme (léame) que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, consulte Uso del ampliador de esquema de Dell.

Puede copiar y ejecutar el ampliador de esquema o los archivos LDIF desde cualquier ubicación.

Uso del ampliador de esquema de Dell

AVISO: Dell Schema Extender usa 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 el ampliador de esquema de Dell.
5. Haga clic en **Finish** (Finalizar).

   El esquema ha sido extendido. Para verificar la ampliación del esquema, use la Consola de administración de Microsoft (MMC) y el complemento de esquema de Active Directory para verificar que existen los siguientes:

   - Clases (consulte de la tabla 6-2 a la tabla 6-7)
   - Atributos (tabla 6-8)

   Consulte la documentación de Microsoft para obtener más información acerca de cómo habilitar y usar el complemento de esquema de Active Directory en el MMC.

Tabla 6-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	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 6-3. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Descripción	Representa el dispositivo RAC de Dell. El dispositivo RAC debe estar configurado como dellRacDevice en Active Directory. Esta configuración hace posible que el iDRAC envíe consultas de Protocolo de acceso ligero de directorio (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 6-4. Clase dellAssociationObject

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	dellProductMembers dellPrivilegeMember

Tabla 6-5. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Se usa para definir los privilegios (derechos de autorización) del dispositivo iDRAC.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

Tabla 6-6. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 6-7. Clas dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 6-8. 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 de dellPrivilege Dell que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Lista de los objetos dellRacDevices que pertenecen a esta función. Este atributo es el vínculo de avance al vínculo de retroceso dellAssociationMembers. Identificación del vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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)	TRUE
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de redirección de consola en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Este atributo es el tipo de RAC actual para el objeto dellRacDevice 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 ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Lista de los miembros de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el eslabón de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Cuando usted amplía el esquema en Active Directory, debe ampliar también el complemento Usuarios y equipos de Active Directory de manera que el administrador pueda controlar los dispositivos de RAC (iDRAC), los usuarios y los grupos de usuarios, las asociaciones de RAC y los privilegios de RAC.

Al instalar el software de administración de sistemas por medio del CD *Dell Systems Management Consoles*, puede ampliar el complemento si selecciona la opción **Extensión de Dell al complemento de usuarios y equipos de Active Directory** durante el proceso de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener más instrucciones sobre la instalación del software de administración de sistemas.

Para 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 de iDRAC de Active Directory. Si no instala Administrator Pack, no podrá ver el objeto RAC de Dell en el contenedor.

Para obtener más información, consulte el apartado Cómo abrir el complemento de usuarios y equipos de Active Directory.

Cómo abrir el complemento de usuarios y equipos de Active Directory

Para abrir el complemento de usuarios y equipos de Active Directory, realice los pasos siguientes:

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

   Si no está conectado en el controlador de dominio, debe tener el Administrator Pack de Microsoft correspondiente instalado en el sistema local. Para instalar este Administrator Pack, haga clic en **Inicio**→ **Ejecutar**, escriba `MMC` y oprima **Entrar**.

   Aparecerá la ventana Consola de administración de Microsoft (MMC).

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).

3. Haga clic en **Agregar o quitar complemento**.

4. Seleccione el complemento **Usuarios y equipos de Active Directory** y haga clic en **Agregar**.

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

Cómo agregar usuarios y privilegios de iDRAC a Active Directory

Con el complemento Usuarios y equipos de Active Directory ampliado por Dell, usted puede agregar usuarios y privilegios del iDRAC mediante la creación de objetos de RAC, de asociación y de privilegio. Para agregar cada tipo de objeto, realice los pasos a continuación:

- Cree un objeto de dispositivo de RAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto de dispositivo de RAC

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

2. Seleccione **Nuevo**→ **Objeto de RAC de Dell**.

   Aparece la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC que usted va a introducir en el paso a de la sección Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web.

4. Seleccione **Objeto de dispositivo de RAC**.

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

Creación de un objeto de privilegio

NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Objeto de RAC de Dell**.

   Aparece 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 RAC** y seleccione los privilegios que desea el usuario tenga (para obtener más información, consulte Privilegios del usuario del iDRAC).

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El ámbito de la asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Cuando cree un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objeto que quiere agregar.

Por ejemplo, si selecciona **Universal** los objetos de asociación sólo estarán disponibles cuando el dominio de Active Directory funcione en el modo nativo o superior.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Objeto de RAC de Dell**.

   Esto abrirá la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de asociación**.
5. Seleccione el ámbito para el **objeto de asociación**.
6. Haga clic en **OK** (Aceptar).

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades de objeto de asociación**, puede asociar a usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta Windows 2000 o posteriores, use los grupos universales para abarcar dominios con los objetos de RAC o usuario.

Puede agregar a grupos de dispositivos de RAC y 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 el **objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de grupo de usuarios o usuario y haga clic en **Aceptar**.

Haga clic en la 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 autentican en un dispositivo RAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

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

Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados con la red que están disponibles para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de RAC a un objeto de asociación.

Cómo agregar dispositivos de RAC o grupos de dispositivos de RAC

Para agregar dispositivos de RAC o grupos de dispositivos de RAC:

1. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
2. Escriba el nombre del dispositivo de RAC o del grupo de dispositivos de RAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web

1. Abra una ventana del explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC.
3. Haga clic en **Sistema**→ **Acceso remoto**.
4. Haga clic en la ficha **Configuración** y seleccione **Active Directory**.
5. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.
6. En la sección Configuración común:
   e. Seleccione la casilla de marcación **Activar Active Directory.**
   f. Escriba el **nombre del dominio raíz**. El **nombre del dominio raíz** es el nombre del dominio raíz completamente calificado para el bosque.
   g. Escriba el **Tiempo de espera** en segundos.
7. Haga clic en **usar esquema ampliado** en la sección Selección del esquema de Active Directory.
8. En la sección Configuración del esquema ampliado:
   a. Escriba el **Nombre de DRAC**. Este nombre debe ser el mismo que el nombre común del nuevo objeto de RAC que creó en el controlador del dominio (consulte el paso 3 de Creación de un objeto de dispositivo de RAC).
   b. Escriba el **Nombre del dominio de iDRAC** (por ejemplo, `iDRAC.com`). No use el nombre de NetBIOS. El **Nombre de dominio del DRAC** es el nombre completo de dominio del subdominio en donde se encuentra el objeto de dispositivo de RAC.
9. Haga clic en **Aplicar** para guardar la configuración de Active Directory.
10. Haga clic en **Volver al menú principal de Active Directory**.
11. Cargue el certificado raíz de CA del bosque de dominio en el iDRAC.
    a. Seleccione el botón de radio **Cargar certificado de CA de Active Directory** y luego haga clic en **Siguiente**.
    b. En la página **Carga del certificado**, escriba la ruta de acceso del archivo del certificado o desplácese al directorio del 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 al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

    Los certificados SSL de los controladores de dominio deberán haber sido firmados por la CA raíz. Tenga el certificado raíz de CA disponible en la estación de administración mientras accede al iDRAC (consulte Exportación del certificado de CA de raíz del controlador de dominio).

    c. Haga clic en **Aplicar**.

    El Web Server de iDRAC se reinicia automáticamente después de que se hace clic en **Aplicar**.
12. Cierre sesión y luego inicie sesión en el iDRAC para completar la configuración del componente Active Directory de iDRAC.
13. Haga clic en **Sistema**→ **Acceso remoto**.

14. Haga clic en la ficha **Configuración** y haga clic en **Red**.

15. Si **Usar DHCP (para la dirección IP del NIC)** está seleccionado en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

    Para introducir manualmente una dirección IP del servidor DNS, deseleccione **Usar DHCP para obtener las direcciones del servidor DNS** y escriba las direcciones IP principal y alternativa del servidor DNS.

16. Haga clic en **Aplicar cambios**.

    Ha concluido la configuración del componente Active Directory de esquema ampliado de iDRAC.

Configuración del iDRAC con Active Directory de esquema ampliado por medio de RACADM

Use los comandos siguientes para configurar el componente Active Directory del iDRAC con el esquema ampliado mediante la CLI de RACADM en vez de la interfaz web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nombre_de_dominio_completo_del_RAC>

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre_de_dominio_raíz_completo>

   racadm config -g cfgActiveDirectory -o cfgADRacName <nombre_común_del_RAC>

   racadm sslcertupload -t 0x2 -f <URI_de_TFTP_del_certificado_raíz_de_CA>

   racadm sslcertdownload -t 0x1 -f <certificado_SSL_del_RAC>
   ```

2. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando RACADM:

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

3. Si el DHCP está deshabilitado en el iDRAC o si desea introducir manualmente las direcciones IP de DNS, escriba los siguientes comandos RACADM:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección_IP_primaria_de_DNS>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección_IP_secundaria_de_DNS>
   ```

4. Presione **Entrar** para completar la configuración del componente Active Directory de iDRAC.

Configuración del iDRAC con Active Directory de esquema ampliado y SM-CLP

NOTA: Se debe tener un servidor TFTP funcionando de donde se pueda recuperar el certificado raíz de CA y en donde se pueda guardar el certificado de servidor del iDRAC.

Use los comandos siguientes de configurar el componente Active Directory del iDRAC con el esquema ampliado por medio de SM-CLP.

1. Inicie sesión en el iDRAC por medio de Telnet o SSH e introduzca los siguientes comandos de SM-CLP:

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=1

   set oemdell_adracdomain=<nombre_de_dominio_completo_del_RAC>

   set oemdell_adrootdomain=<nombre_de_dominio_raíz_completo>

   set oemdell_adracname=<nombre_común_del_RAC>

   set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD

   load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1
   ```

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <URI_de_TFTP_de_certificado_de_servidor_del_DRAC> /system1/sp1/oemdell_ssl1
```

2. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando de SM- CLP:

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdell_serversfromdhcp=1
```

3. Si el DHCP está deshabilitado en el iDRAC o si desea introducir manualmente la dirección IP de DNS, escriba los siguientes comandos de SM-CLP:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_de_ DNS_ primaria>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_de_ DNS_ secundaria>
```

Descripción del esquema estándar de Active Directory

Como se muestra en la figura 6-4, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en el iDRAC. En Active Directory, se usa un objeto de grupo estándar como grupo de funciones. Los usuarios que tengan acceso al iDRAC serán miembros del grupo de funciones. Para dar acceso a tales usuarios a un iDRAC específico, el nombre del grupo de funciones y el nombre de dominio del mismo deberán estar configurados en el iDRAC específico. A diferencia de la solución de esquema ampliado, la función y el nivel de privilegios se definen en cada iDRAC y no en Active Directory. Se pueden configurar y definir hasta cinco grupos de funciones en cada iDRAC. La tabla 5-10 muestra el nivel de privilegios de los grupos de funciones y la tabla 6-9 muestra la configuración predeterminada del grupo de funciones.

Figura 6-4. Configuración del iDRAC con Microsoft Active Directory y el esquema estándar

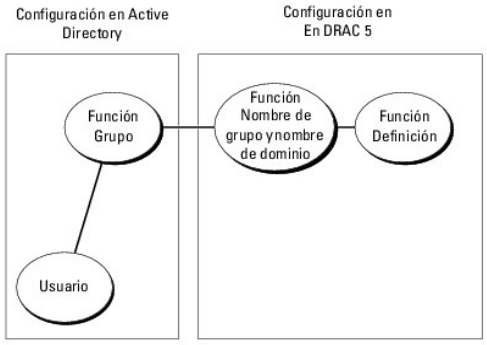


Tabla 6-9. Privilegios predeterminados del grupo de funciones

Nivel predeterminado de privilegios	Permisos concedidos	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 redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**	0x000001ff
Usuario avanzado	**Iniciar sesión en el** iDRAC, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**	0x000000f9
Usuario invitado	Inicio de sesión en iDRAC	0x00000001
Ninguno	Sin permisos asignados	0x00000000
Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits sólo se usan cuando se configura el esquema estándar con RACADM.

Hay dos maneras de habilitar el esquema estándar en Active Directory:

- Con la interfaz de usuario web del iDRAC. Consulte el apartado Configuración del iDRAC con Active Directory de esquema estándar y la interfaz web.
- Con la herramienta de CLI de RACADM. Consulte el apartado Configuración del iDRAC con Active Directory de esquema estándar y RACADM.

Configuración de Active Directory de esquema estándar para acceder al iDRAC

Usted debe realizar los pasos a continuación para configurar Active Directory antes de que los usuarios de Active Directory puedan acceder al iDRAC:

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. Se deberán configurar el nombre del grupo y el nombre de este dominio en el iDRAC con la interfaz web, RACADM o SM-CLP (consulte Configuración del iDRAC con Active Directory de esquema estándar y la interfaz web o Configuración del iDRAC con Active Directory de esquema estándar y RACADM).

3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para que pueda tener acceso al iDRAC.

Configuración del iDRAC con Active Directory de esquema estándar y la interfaz web

1. Abra una ventana del explorador web compatible.

2. Inicie sesión en la interfaz web del iDRAC.

3. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y después haga clic en la ficha **Configuración**.

4. Seleccione **Active Directory** para abrir la página **Menú principal de Active Directory**.

5. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.

6. En la sección Configuración común:

   a. Seleccione la casilla de marcación **Activar Active Directory**.

   b. Escriba el **nombre del dominio raíz**. El **nombre del dominio raíz** es el nombre del dominio raíz completamente calificado para el bosque.

   c. Escriba el **Tiempo de espera** en segundos.

7. Haga clic en **usar esquema ampliado** en la sección Selección del esquema de Active Directory.

8. Haga clic en **Aplicar** para guardar la configuración de Active Directory.

9. En la columna **Grupos de funciones** de la sección de configuración del esquema estándar, haga clic en un **Grupo de funciones**.

   Aparecerá la página **Configurar grupo de funciones**, que incluye el **Nombre de grupo**, **Dominio de grupo** y **Privilegios del grupo de funciones** del grupo de funciones.

10. Escriba el **Nombre de grupo**. El nombre de grupo que identifica el grupo de funciones en Active Directory relacionado con el iDRAC.

11. Escriba el **Dominio de grupo**. El **Nombre de grupo** es el nombre completo del dominio raíz para el bosque.

12. En la página **Privilegios del grupo de funciones**, defina los privilegios del grupo.

    La tabla 5-10 describe los **Privilegios del grupo de funciones**.

    Si modifica alguno de los permisos, el **Privilegio del grupo de funciones** existente (**Administrador**, **Usuario Avanzado** o **Usuario invitado**) cambiará al grupo Personalizado o al **Privilegio de grupo de funciones** correspondiente según los permisos que se modifiquen.

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

14. Haga clic en **Volver a la configuración y administración de Active Directory**.

15. Haga clic en **Volver al menú principal de Active Directory**.

16. Cargue el certificado raíz de CA del bosque de dominio en el iDRAC.

    a. Seleccione el botón de radio **Cargar certificado de CA de Active Directory** y luego haga clic en **Siguiente**.

    b. En la página **Carga del certificado**, escriba la ruta de acceso del archivo del certificado o desplácese al directorio del 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 al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

    Los certificados SSL de los controladores de dominio deberán haber sido firmados por la CA raíz. Tenga el certificado raíz de CA disponible en la estación de administración mientras accede al iDRAC (consulte Exportación del certificado de CA de raíz del controlador de dominio).

    c. Haga clic en **Aplicar**.

    El Web Server de iDRAC se reinicia automáticamente después de que se hace clic en **Aplicar**.

17. Cierre sesión y luego inicie sesión en el iDRAC para completar la configuración del componente Active Directory de iDRAC.

18. Haga clic en **Sistema**→ **Acceso remoto**.

19. Haga clic en la ficha **Configuración** y haga clic en **Red**.

20. Si **Usar DHCP (para la dirección IP del NIC)** está seleccionado en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

    Para introducir manualmente una dirección IP del servidor DNS, deseleccione **Usar DHCP para obtener las direcciones del servidor DNS** y escriba las direcciones IP principal y alternativa del servidor DNS.

21. Haga clic en **Aplicar cambios**.

    Ha concluido la configuración del componente Active Directory de esquema estándar de iDRAC.

Configuración del iDRAC con Active Directory de esquema estándar y RACADM

Use los comandos siguientes para configurar el componente Active Directory del iDRAC con el esquema estándar mediante la CLI de RACADM en vez de la interfaz web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre_de_dominio_raíz_completo>

   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_del_RAC>

   racadm config -g cfgStandardSchema -i <índice> -o cfgSSADRoleGroupPrivilege <máscara_de_bits_de_permisos>

   racadm sslcertupload -t 0x2 -f <URI_de_TFTP_del_certificado_raíz_de_CA>

   racadm sslcertdownload -t 0x1 -f <URI_de_TFTP_del_certificado_SSL_del_RAC>
   ```

   NOTA: Para obtener los valores de máscara de bits, consulte la tabla B-1.

2. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba los siguientes comandos RACADM:

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

3. Si el DHCP está deshabilitado en el iDRAC o si usted 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_primaria_de_DNS>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección_IP_secundaria_de_DNS>
   ```

Configuración del iDRAC con Active Directory de esquema estándar y SM-CLP

NOTA: No se pueden cargar certificados por medio de SM-CLP. En vez de ello, use la interfaz web del iDRAC o comandos de RACADM local.

Use los siguientes comandos para configurar el componente Active Directory de iDRAC con el esquema estándar por medio de SM-CLP.

1. Inicie sesión en el iDRAC por medio de Telnet o SSH e introduzca los siguientes comandos de SM-CLP:

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=2

   set oemdell_adracdomain=<nombre_de_dominio_completo_del_RAC>
   ```

2. Introduzca los comandos siguientes para cada uno de los cinco grupos de funciones de Active Directory:

   ```
   set /system1/sp1/groupN oemdell_groupname=<nombre_común_del_grupoN_de_funciones>
   ```

```
set /system1/sp1/groupN oemdell_groupdomain=<FQDN_del_RAC>

set /system1/sp1/groupN oemdell_groupprivilege=<máscara_de_bits_de_permiso_de_usuario>
```

donde *N* es un número de 1 a 5.

3. Introduzca los comandos siguientes para instalar las certificaciones de SSL de Active Directory.

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1

set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL

dump -destination <URI_de_TFTP_de_certificado_de_servidor_del_iDRAC> /system1/sp1/oemdell_ssl1
```

4. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando de SM- CLP:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=1
```

5. Si el DHCP está deshabilitado en el iDRAC o si desea introducir manualmente las direcciones IP de DNS, escriba los siguientes comandos de SM-CLP:

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_de_ DNS_ primaria>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_de_ DNS_ secundaria>
```

Activación de SSL en un controlador de dominio

Si está usando la autoridad de certificados raíz de empresa de Microsoft para asignar automáticamente todos controladores de dominio a un certificado SSL, realice los pasos siguientes para habilitar SSL en cada controlador de dominio.

1. Instale una CA de raíz de Microsoft Enterprise en un controlador de dominio.
   a. Seleccione **Inicio**→ **Panel de control**→ **Agregar o quitar programas**.
   b. Seleccione **Agregar o quitar componentes de Windows**.
   c. En el **Asistente de componentes de Windows**, seleccione la casilla **Servicios de certificado**.
   d. Seleccione **CA de raíz de Enterprise** como **Tipo de CA** y haga clic en **Siguiente**.
   e. Introduzca un **Nombre común para esta CA**, haga clic en **Siguiente** y luego en **Terminar**.
2. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Política de seguridad del dominio**.
   b. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   c. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado de CA de raíz del controlador de dominio

NOTA: Si el sistema ejecuta Windows 2000, 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 en **Consola** en sistemas con Windows 2000) y seleccione **Agregar o quitar complemento**.
5. En la ventana **Agregar o 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. Ubique el certificado raíz de CA y haga clic con el botón derecho del mouse en el mismo, seleccione **Todas las tareas** y **haga clic en Exportar...**.
12. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
15. Cargue el certificado que guardó en el iDRAC en el paso 14.

    Para cargar el certificado por medio de RACADM, consulte Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web.

    Para cargar el certificado por medio de la interfaz web, realice el procedimiento siguiente:

    a. Abra una ventana del explorador web compatible.
    b. Inicie sesión en la interfaz web del iDRAC.
    c. Haga clic en **Sistema**→ **Acceso remotoÆ** iDRAC y después haga clic en la ficha Configuración.
    d. Haga clic en **Seguridad** para abrir la página **Menú principal del certificado de seguridad**.
    e. En la página **Menú principal de certificado de seguridad**, seleccione **Cargar certificado de servidor** y haga clic en **Aplicar**.
    f. En la pantalla **Carga de un certificado**, realice uno de los pasos siguientes:
        - Haga clic en **Examinar** y seleccione el certificado.
        - En el campo **Valor**, escriba la ruta de acceso del certificado.
    g. Haga clic en **Aplicar**.

Cómo importar el certificado SSL de firmware de iDRAC

Use el procedimiento siguiente para importar el certificado SSL de firmware de iDRAC 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 de iDRAC está firmado por una autoridad de certificados reconocida, no necesita realizar los pasos descritos en esta sección.

El certificado SSL de iDRAC es el certificado idéntico que se usa para el Web Server de iDRAC. Todos los iDRAC se envían con un certificado predeterminado autofirmado.

Para acceder al certificado por medio de la interfaz web del iDRAC, seleccione **Configuración**→ **Active Directory**→ **Descargar el certificado de servidor del iDRAC**.

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 RAC en la **Autoridad de certificación de raíz confiable** de cada controlador de dominio.

   Si ha instalado su propio certificado, asegúrese que la CA que firma su certificado esté en la lista **Autoridad de certificación de raíz confiable**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.
5. Haga clic en **Siguiente** y seleccione si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o desplácese a un almacén de su elección.
6. Haga clic en **Terminar** y luego en **Aceptar**.

Uso de Active Directory para iniciar sesión en el iDRAC

Usted puede usar Active Directory para iniciar sesión en el iDRAC por medio de la interfaz web. Use uno de los formatos siguientes para introducir el nombre de usuario:

<nombre_de_usuario@dominio>

O bien:

<dominio>\<nombre_de_usuario>

O bien:

<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.

Preguntas más frecuentes

La tabla 6-10 contiene las preguntas y respuestas frecuentes.

Tabla 6-10. Uso de iDRAC con Active Directory: Preguntas frecuentes Preguntas

Question	Answer
¿Puedo iniciar sesión en el iDRAC usando Active Directory entre varios árboles?	Sí El algoritmo de consulta de Active Directory del iDRAC admite varios árboles en un solo bosque.
¿El inicio de sesión en el iDRAC por medio de Active Directory funciona en el modo mixto (es decir, los controladores de dominio en el bosque ejecutan distintos sistemas operativos, como Microsoft Windows NT® 4.0, Windows 2000 o Windows Server 2003)?	Sí En el modo mixto, todos los objetos que el proceso de consulta de iDRAC usa (entre usuario, objeto de dispositivo del RAC y objeto de asociación) tienen que estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory ampliado por Dell verifica el modo y limita a los usuarios a fin de crear objetos a través de dominios si se encuentra en modo mixto.
¿El uso de iDRAC con Active Directory admite varios entornos de dominio?	Sí El nivel de función del bosque de dominio debe estar en modo Nativo o en modo de Windows 2003. Además, los grupos entre objeto de asociación, objetos de usuario de RAC, y objetos de dispositivo de RAC (incluso el objeto de asociación) deben ser grupos universales.
¿Estos objetos ampliados por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?	El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory ampliado por Dell le obliga a crear estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes.
¿Hay alguna restricción para la configuración del controlador de dominio de SSL?	Sí Todos los certificados SSL de los servidores de Active Directory en el bosque deben estar firmados por la misma CA raíz pues el iDRAC sólo permite cargar un certificado SSL de CA de confianza.
Creé y cargué un nuevo certificado de RAC y ahora la interfaz web no se inicia.	Si usa servicios de Certificate Server de Microsoft para generar el certificado de RAC, una causa posible de esto es que haya elegido por descuido **Certificado de usuario** en vez de **Certificado de web** al crear el certificado. Para recuperarse de esto, genere una CSR y después cree un nuevo certificado de web a partir de los servicios de Certificate Server de Microsoft y cárguelo a través de la CLI de RACADM desde el servidor administrado con los siguientes comandos de RACADM: racadm sslcsrgen [-g] [-u] [-f {nombre_de_archivo}] racadm sslcertupload -t 1 -f {cert_SSL_de_web}
¿Qué puedo hacer si no puedo iniciar sesión en el iDRAC mediante la autentificación de Active Directory? ¿Cómo soluciono el problema?	1. Asegúrese de usar el nombre de dominio de usuario correcto durante un inicio de sesión y no el nombre de NetBIOS. 2. Si tiene una cuenta de usuario local de iDRAC, inicie sesión en el iDRAC usando las credenciales locales. Después de que haber iniciado sesión, realice los pasos a continuación: a. Asegúrese de haber marcado la casilla **Habilitar Active Directory** en la página **Configuración de Active Directory** de iDRAC. b. Asegúrese que la configuración del DNS sea correcta en la página **Configuración de la red** de iDRAC. c. Asegúrese de haber cargado en el iDRAC el certificado de Active Directory que provino de la autoridad de certificados raíz de Active Directory. d. Revise los certificados de SSL de controlador de dominio para asegurarse que no hayan expirado. e. Asegúrese que **Nombre del DRAC**, **Nombre del dominio raíz** y **Nombre del dominio de DRAC** coincidan con la configuración de entorno de Active Directory. f. Asegúrese que la contraseña de iDRAC tenga un máximo de 127 caracteres. Si bien el iDRAC puede admitir contraseñas de hasta 256 caracteres, Active Directory sólo admite contraseñas con un máximo de 127 caracteres.

Regresar a la página de contenido

Regresar a la página de contenido

Visualización de la configuración y la condición del servidor administrado

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Resumen del sistema

Haga clic en **Sistema**→ **Propiedades**→ **Resumen** para obtener información acerca del Gabinete del sistema principal y el Integrated Dell Remote Access Controller.

Gabinete del sistema principal

Información del sistema

Esta sección de la interfaz web de iDRAC suministra la siguiente información acerca del servidor administrado:

- Descripción: el número de modelo o el nombre del servidor administrado.
- Versión BIOS: el número de versión del BIOS del servidor administrado.
- Etiqueta de servicio: el número de etiqueta de servicio del servidor administrado.
- Nombre del host: el nombre del host DNS asociado con el servidor administrado.
- Nombre OS: el nombre del sistema operativo instalado en el servidor administrado.

Tarjeta intermedia E/S

Esta sección de la interfaz web iDRAC brinda la siguiente información acerca de las tarjetas intermedias E/S y las tarjeta de controlador de almacenamiento instaladas en el servidor administrado:

- Tarjeta intermedia ES: presenta una lista de todas las tarjetas intermedias E/S instaladas en el servidor administrado.
- Tipo de tarjeta: el tipo físico de tarjeta/conexión intermedia instalada.
- Nombre del modelo: el número, tipo o descripción del modelo de la(s) tarjeta(s) intermedia(s) instalada(s).
- Tarjeta de almacenamiento integrada: el número o nombre del modelo de la tarjeta de controlador de almacenamiento instalada.

Autorecuperación

Esta sección de la interfaz web iDRAC detalla el modo de operación actual de la función de autorecuperación del servidor administrado según la configuración del administrador del servidor Open Manage:

- Acción de recuperación: acción a realizar cuando se detecta una falla o *bloqueo* en el sistema. Las acciones disponibles son **Ninguna acción**, **Restablecimiento forzado**, **Apagar** o **Ciclo de encendido**.
- Cuenta regresiva inicial: la cantidad de tiempo (en segundos) después de la detección de un bloqueo de sistema en que el iDRAC realiza una acción de recuperación.
- Cuenta regresiva actual: el valor actual (en segundos) del temporizador.

Integrated Dell Remote Access Controller

Información iDRAC

Esta sección de la interfaz web de iDRAC suministra la siguiente información acerca del servidor administrado:

- Fecha/hora: la fecha y hora actual (del momento de la última actualización de la página) del iDRAC.
- Versión de firmware: la versión actual del firmware instalada en el servidor administrado.
- Actualización del firmware: la fecha y hora de la última actualización exitosa del firmware de iDRAC.

- Versión del hardware: el número de versión del plano primario (placa de circuito) del servidor administrado.
- Dirección IP: la dirección IP asociada con el iDRAC (no el servidor administrado).
- Puerta de enlace: la dirección IP de la puerta de enlace de red configurada para el iDRAC.
- Máscara de subred: la máscara de subred TCP/IP configurada para el iDRAC.
- Dirección MAC: la dirección MAC asociada con el controlador de interfaz de red de LOM (LAN de la placa base) del iDRAC.
- DHCP activado: activado si el iDRAC está configurado para tomar su dirección IP e información asociada de un servidor DHCP.
- Dirección DNS preferida 1: configurada para el servidor DNS primario activo actual.
- Dirección DNS alternativa 2: configurada para el servidor DNS alternativo.

NOTA: Esta información también está disponible en **iDRAC**→ **Propiedades**→ **Información iDRAC**.

Resumen WWN/MAC

Haga clic en **Sistema**→ **Propiedades**→ **WWN/MAC** para ver la configuración actual de las tarjetas intermedias E/S y sus redes fabric asociadas. Si la función FlexAddress está activada, las direcciones MAC persistentes asignadas globalmente (asignado al chasis) reemplazarán a los valores de cableado de cada LOM.

Condición del sistema

Haga clic en **Sistema**→ **Propiedades**→ **Condición** para visualizar la información importante acerca de la condición del iDRAC y los componentes supervisados por el iDRAC. La columna **Gravedad** muestra el estado para cada componente. Para obtener una lista de símbolos de estado y su significado, consulte tabla 14-3. Haga clic en el nombre del componente en la columna **Componente** para obtener información más detallada acerca del componente.

NOTA: La información del componente también puede obtenerse con un clic sobre el nombre del componente en el panel izquierdo de la ventana. Los componentes permanecen visibles en el panel izquierdo independientemente de la ficha/pantalla seleccionada.

iDRAC

La página de información iDRAC presenta una lista de detalles importantes acerca del iDRAC, como el estado de la condición, nombre, revisión de firmware y parámetros de red. Se puede acceder a los detalles adicionales haciendo clic sobre la ficha correspondiente al inicio de la página.

CMC

La página CMC muestra el estado de condición, revisión de firmware y dirección IP del Chassis Management Controller. También puede iniciar la interfaz web con un clic sobre el botón **Iniciar la interfaz web CMC**.

Baterías

La página de baterías muestra el estado y valores de la batería plana de la placa de sistema que mantiene el reloj en tiempo real (RTC) y el almacenamiento de los datos de configuración CMOS del sistema administrado.

Temperaturas

La página de información de sondas de temperatura muestra el estado y las lecturas de la sonda de temperatura ambiente integrada. Se muestran los umbrales de temperatura mínima y máxima para *advertencia* o *falla*, junto con el estado de condición actual de la sonda.

Voltajes

La página de información de sonda de voltaje muestra el estado y la lectura de las sondas de voltaje y suministra información como el estado del riel de voltaje incorporado y los sensores de núcleo de CPU.

NOTA: Dependiendo del modelo de su servidor, puede que los umbrales de temperatura para los estados *advertencia* o *falla* y/o estado de condición de la sonda no se visualicen.

Supervisión de alimentación

La página de supervisión de alimentación le permite ver la siguiente información de supervisión y estadísticas de alimentación:

- Supervisión de alimentación: muestra la cantidad de energía que usa (en watts) el servidor según lo informado por el Monitor actual de la placa de sistema.

- Estadísticas de seguimiento de alimentación: muestra la información acerca de la cantidad de alimentación utilizada por el sistema desde el último restablecimiento de la **Hora inicial de medición**.
- Estadísticas pico: muestra la información acerca de la cantidad pico de alimentación utilizada por el sistema desde el último restablecimiento de la **Hora inicial de medición**.

CPU

La página de información de CPU informa la condición de cada CPU en el servidor administrado. Este estado de condición es un resumen de pruebas individuales térmicas, funcionales y de alimentación.

POST

La página de Código Post muestra el último código post del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.

Condiciones diversas

La página Condiciones diversas suministra acceso a los siguientes registros del sistema:

Registros de sucesos del sistema: muestra los sucesos críticos de sistema que se producen en el sistema administrado.

Código Post: muestra el último código post del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.

Último bloqueo: muestra la pantalla y la hora de bloqueo más recientes.

Captura de inicio: brinda una reproducción de las últimas tres pantallas de inicio.

NOTA: Esta información también está disponible en **Sistema**→ **Propiedades**→ **Registros**.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la redirección de consola con interfaz gráfica de usuario

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Esta sección proporciona información acerca de cómo usar la función de redirección de consola de iDRAC.

Información general

La función de redirección de consola de iDRAC le permite tener acceso a la consola del servidor local de manera remota en modos de gráficos o de texto. Por medio de la redirección de consola, puede controlar uno o varios sistemas equipados con iDRAC desde una ubicación.

No es necesario ir personalmente a cada servidor para realizar todo el mantenimiento de rutina. En vez de eso, usted puede administrar los servidores desde donde se encuentre, desde su equipo de escritorio o desde su equipo portátil. También puede compartir la información con otros; de manera remota e instantánea.

Uso de redirección de consola

NOTA: Cuando usted abre una sesión de redirección de consola, el servidor administrado no indica que la consola ha sido redirigida.

La página **Redirección de consola** permite administrar el sistema remoto con el teclado, vídeo y mouse en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta característica puede ser usada junto con la característica de medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- Sólo se admite un máximo de dos sesiones simultáneas de redirección de consola. Ambas sesiones muestran la misma consola de servidor administrado simultáneamente.
- La sesión de redirección de consola no se deberá ejecutar desde un explorador web en el sistema administrado.
- Se requiere un ancho de banda disponible de red de 1 MB/s.

Si un segundo usuario solicita una sesión de redirección de consola, el primer usuario recibe una notificación y se brinda la opción de rechazar el acceso, permitir sólo vídeo o permitir el acceso compartido completo. El segundo usuario es notificado que otro usuario tiene el control. El primer usuario debe responder en treinta segundos o se otorgará automáticamente el acceso completo al segundo usuario. Durante ese tiempo hay dos sesiones activas de forma simultánea, cada usuario ve un mensaje en la esquina superior derecha de la pantalla que identifica otro usuario con sesión activa. No se permite una tercera sección activa. Si un tercer usuario solicita una sesión de redirección de la consola, se deniega el acceso sin interrumpir las sesiones del primer y segundo usuario.

Si ni el primer ni el segundo usuario tienen privilegios de administrador, la finalización de la sección activa del primer usuario finaliza también la sesión del segundo usuario.

Resoluciones de pantalla y velocidades de actualización admitidas

La tabla 8-1 muestra una lista de las resoluciones admitidas de pantalla y las velocidades de actualización correspondientes para una sesión de redirección de consola que se ejecuta en el servidor administrado.

Tabla 8-1. 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 estación de administración

Para usar la redirección de consola en la estación de administración, realice los siguientes procedimientos:

1. Instale y configure un explorador de web admitido. Consulte las siguientes secciones para obtener más información:
   - Exploradores web admitidos
   - Configuración de un explorador de web admitido
2. Si usa Firefox o desea usar el visor de Java con Internet Explorer, instale Java Runtime Environment (JRE). Consulte el apartado Instalación de Java Runtime Environment (JRE).
3. Se recomienda que configure la resolución del monitor en 1280 x 1024 pixeles o más.

AVISO: Si tiene una sesión de redirección de consola activa y hay un monitor de menor resolución conectado con el iKVM, la resolución de la consola del servidor puede restablecerse si el servidor se selecciona en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iKVM, Linux cambiará a consola de texto.

Configuración de la redirección de consola en la interfaz web del iDRAC

Para configurar la redirección de consola en la interfaz web del iDRAC, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Consola**.
2. Haga clic en **Configuración** para abrir la página **Configuración de la redirección de consola**.
3. Configure las propiedades de la redirección de consola. La tabla 8-2 describe la configuración de la redirección de consola.
4. Cuando termine, haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 8-3.

Tabla 8-2. Propiedades de configuración de la redirección de consola

Propiedad	Descripción
Activado	Haga clic para activar o desactivar la Redirección de consola. **Seleccionado** indica que la redirección de consola está activada. **Deseleccionado** indica que la redirección de consola está desactivada. El valor predeterminado es **activado**.
Nº. máx. de sesiones	Muestra el número máximo posible de sesiones de redirección de consola, **1** ó **2**. Use el menú desplegable para cambiar el número máximo posible de sesiones de Redirección de consola. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de Consola activa. Este campo es de sólo lectura.
Número del puerto de teclado y mouse	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es **5900**.
Número del puerto de vídeo	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Se recomienda cambiar este valor si otro programa está usando el puerto predeterminado. El valor predeterminado es **5901**.
Cifrado de vídeo activado	**Seleccionado** indica que el cifrado de vídeo está activado. Todo el tráfico 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.**
Modo Mouse	Elija **Windows** cuando el servidor administrado se esté ejecutando en un sistema operativo Windows. Elija **Linux** si el servidor ejecuta Linux. Elija **Ninguno** cuando el servidor se esté ejecutando en un sistema operativo que no sea Windows ni Linux. El valor predeterminado es **Windows**.
Tipo de complemento de la consola para IE	Cuando use Internet Explorer en un sistema operativo Windows, puede elegir entre los siguientes visores: *ActiveX*: el visor *ActiveX para redirección de consola* Java: el visor *Java para Redirección de consola*. **NOTA:** Dependiendo de la versión de Internet Explorer, deberá desactivar restricciones de seguridad adicionales (consultar Configuración y uso de medios virtuales). **NOTA:** Deberá tener instalado Java Runtime Environment en el sistema cliente a fin de usar el visor de Java.
Desactivar consola local	Si está seleccionado, indica que la salida al monitor iKVM está desactivada durante la redirección de consola. Esto garantiza que las tareas que realice usando **Redirección de consola** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte Configuración y uso de medios virtuales.

Los botones en la tabla 8-5 están disponibles en la página **Configuración de la redirección de consola**.

Tabla 8-3. Botones de la página de configuración de la redirección de consola

Botón	Definición
Imprimir	Imprime la página **Configuración de la redirección de consola**
Actualizar	Actualiza la página **Configuración de la redirección de consola**
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la redirección de consola.

Configuración de la redirección de consola en la interfaz de línea de comandos de SM-CLP

Abrir una sesión de redirección de consola

Cuando abre una sesión de redirección de consola, la aplicación Dell Virtual KVM Viewer se inicia y aparece el escritorio del sistema remoto en el visor. Al usar la aplicación Virtual KVM Viewer, puede controlar las funciones de mouse y teclado del sistema remoto desde la estación de administración local.

Para abrir una sesión de redirección de consola en la interfaz web, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Consola**.
2. En la página **Redirección de consola**, use la información de la tabla 8-4 para garantizar que haya una sesión de redirección de consola disponible.

   Si desea reconfigurar los valores de las propiedades que se muestran, consulte Configuración de la redirección de consola en la interfaz web del iDRAC.

Tabla 8-4. Información de la página de redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No
Cifrado de vídeo activado	Sí/No
Nº. máx. de sesiones	Muestra el número máximo de sesiones de redirección de consola admitidas
Sesiones actuales	Muestra el número actual de sesiones activas de redirección de consola
Modo Mouse	Muestra la aceleración actual del mouse. El modo de **Aceleración del mouse** se debe elegir con base en el tipo de sistema operativo instalado en el servidor administrado.
Tipo de complemento de consola	Muestra el tipo de complemento actualmente configurado. **ActiveX**: se iniciará un visor Active-X. El visor Active-X únicamente funciona en Internet Explorer cuando se ejecuta en un sistema operativo Windows. **Java**: se iniciará un visor Java. El visor Java se puede usar en cualquier explorador incluso Internet Explorer. Si el cliente se ejecuta en un sistema operativo que no sea Windows, entonces debe usar el visor Java. Si está accediendo al iDRAC desde Internet Explorer ejecutando un sistema operativo Windows, puede elegir el tipo de complemento ya sea ActiveX o Java.
Consola local	Estará deseleccionado si la consola local no ha sido desactivada. Si se selecciona, los usuarios que usen la conexión iKVM en el chasis no podrán acceder a la consola.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte Configuración y uso de medios virtuales.

Los botones en la tabla 8-5 están disponibles en la página **Redirección de consola**.

Tabla 8-5. Botones de la página de redirección de consola

Botón	Definición
Actualizar	Actualiza la página **Configuración de la redirección de consola**
Iniciar el visor	Abre una sesión de redirección de consola en el sistema remoto de destino
Imprimir	Imprime la página **Configuración de la redirección de consola**

3. Si hay una sesión de redirección de consola disponible, haga clic en **Iniciar el visor**.

NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

NOTA: Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información en la ventana y haga clic en **Sí** para seguir.

La estación de administración se conecta al iDRAC y la pantalla de escritorio del sistema remoto aparecerá en la aplicación Dell Digital KVM Viewer.

4. Aparecerán dos apuntadores de mouse en la ventana del visor: uno para el sistema remoto y otro para el sistema local. Usted deberá sincronizar los dos apuntadores del mouse de manera que el apuntador del mouse remoto siga el apuntador del mouse local. Consulte el apartado Sincronización de los apuntadores del mouse.

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver la pantalla de escritorio del servidor administrado y controlar las funciones de mouse y teclado desde la estación de administración. Cuando se conecta con el sistema remoto, Video Viewer se inicia en otra ventana.

Video Viewer proporciona varios ajustes de control, por ejemplo, modo de color, sincronización del mouse, instantáneas, macros de teclado y acceso a los medios virtuales. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Cuando usted inicia una sesión de redirección de consola y Video Viewer aparece, es posible que deba ajustar el modo de color y sincronizar los apuntadores de mouse.

La tabla 8-6 describe las opciones del menú que están disponibles en el visor.

Tabla 8-6. Selecciones de la barra de menú del visor

Elemento del menú	Elemento	Descripción
Vídeo	Pausa	Pausa la redirección de consola temporalmente.
	Reanudar	Reanuda la redirección de consola.
	Actualizar	Vuelve a trazar la imagen de la pantalla del visor.
	Capturar la pantalla actual	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.
	Pantalla completa	Para expandir el Video Viewer al modo de pantalla completa, seleccione **Pantalla completa** desde el menú **Vídeo**.
	Salir	Cuando haya terminado de usar la consola y haya cerrado la sesión (mediante el procedimiento de desconexión del sistema remoto), haga clic en **Salir** desde el menú **Vídeo** para cerrar la ventana del **Video Viewer**.
Keyboard (Teclado)	Mantener presionada la tecla Alt derecha	Seleccione este elemento antes presionar las teclas que desea combinar con la tecla <Alt> derecha.
	Mantenga presionada la tecla Alt izquierda	Seleccione este elemento antes de presionar las teclas que desea combinar con la tecla <Alt> izquierda.
	Tecla Windows izquierda	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows izquierda. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows izquierda.
	Tecla Windows derecha	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows derecha. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows derecha.
	Macros	Cuando selecciona una macro, o presiona la tecla aceleradora especificada para la macro, la acción se ejecuta en el sistema remoto. El Video Viewer ofrece las macros a continuación: • Ctrl-Alt-Supr • Alt-Tab • Alt-Esc • Ctrl-Esc • Alt-Espacio • Alt-Entrar • Alt-Guión • Alt-F4 • ImprPant • Alt-ImprPant • F1 • Pausa • Alt+m
	Paso a través de teclado	El modo de paso a través de teclado permite que todas las funciones del teclado en el cliente se redirijan al servidor.
Mouse	Sincronizar el cursor	El menú **Mouse** permite sincronizar el cursor de modo que el mouse en el cliente se redirija al mouse en el servidor.
Opciones	Modo de color	Permite seleccionar la profundidad del color para mejorar el rendimiento en la red. Por ejemplo, si va a instalar software a partir de medios virtuales, puede seleccionar la profundidad en color más baja (gris de 3 bits), de manera que el visor de consola use menos ancho de banda y se destine mayor ancho de banda a la transferencia de datos de los medios. El modo de color se puede definir en color de 15 bits, color de 7 bits, color de 4 bits, gris de 4 bits y gris de 3 bits.
Medios	Asistente de medios virtuales	El menú **Medios** ofrece acceso al Asistente de medios virtuales, el cual permite redirigir a un dispositivo o imagen, por ejemplo: • Unidad de disco flexible

		▪ CD ▪ DVD ▪ Imagen en formato ISO ▪ Unidad flash USB Para obtener información sobre la función de medios virtuales, consulte Configuración y uso de medios virtuales. Se debe mantener activa la ventana del visor de consola cuando se usan los medios virtuales.
ayuda	N/D	Activa el menú **Ayuda**.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema PowerEdge remoto usando la redirección de consola, la velocidad de aceleración del mouse en el sistema remoto podría no sincronizarse con el apuntador del mouse en la estación de administración, ocasionando que aparezcan dos apuntadores de mouse en la ventana de Video Viewer.

Para sincronizar los apuntadores de mouse, haga clic en **Mouse**→ **Sincronizar el cursor** o presione <Alt><M>.

La opción del menú Sincronizar el cursor es un interruptor. Asegúrese que haya una marca a un lado de la opción del menú; esto indica que la sincronización del mouse está activada.

Cuando se usa Red Hat® Linux® o Novell® SUSE® Linux, asegúrese de configurar el modo de mouse para Linux antes de iniciar el visor. Consulte Configuración de la redirección de consola en la interfaz web del iDRAC para obtener ayuda con la configuración. La configuración predeterminada de mouse del sistema operativo se usa para controlar la flecha del mouse en la pantalla de redirección de consola del iDRAC.

Desactivación o activación de la consola local

Usted puede configurar el iDRAC para rechazar conexiones de iKVM por medio de la interfaz web del iDRAC. Cuando la consola local está desactivada, aparece un punto amarillo de estado en la lista de servidores (OSCAR) para indicar que la consola está bloqueada en el iDRAC. Cuando la consola local está activada, el punto de estado es verde.

Si desea asegurarse que tiene acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local *y reconfigurar el* **Nº. máx. de sesiones** como 1 en la **Página de redirección de consola**.

NOTA: La función de consola local es compatible con todos los sistemas PowerEdge x9xx, excepto los PowerEdge SC1435 y 6950.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, se desactivarán el monitor, teclado y mouse que están conectados al iKVM.

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 iDRAC. Para obtener más información, consulte el apartado Acceso a la interfaz web.
2. Haga clic en **Sistema**, haga clic en la ficha **Consola** y después haga clic en **Configuración**.
3. Si desea desactivar (apagar) el vídeo local en el servidor, en la página **Configuración de la redirección de consola**, seleccione la casilla **Desactivar la consola local** y después haga clic en **Aplicar**. El valor predeterminado es **Apagado**.
4. Si desea activar (encender) el vídeo local en el servidor, en la página **Configuración de la redirección de consola**, deseleccione la casilla **Desactivar la consola local** y después haga clic en **Aplicar**.

La página **Redirección de consola** muestra el estado del vídeo del servidor local.

Preguntas más frecuentes

La tabla 8-7 contiene las preguntas y respuestas frecuentes.

Tabla 8-7. Uso de la redirección de consola: Preguntas frecuentes

Question	Answer
¿Se puede iniciar una nueva sesión de vídeo de consola remota cuando el vídeo local del servidor está apagado?	Sí
¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del vídeo local?	Esto brinda al usuario local la oportunidad de realizar alguna acción antes de que el vídeo se apague.
¿Hay algún retraso al encender el vídeo local?	No, una vez que el iDRAC recibe la solicitud de **encendido** del vídeo local, este último se enciende instantáneamente.
¿El usuario local también puede apagar el vídeo?	Sí, el usuario local puede usar la CLI de RACADM local para apagar el vídeo.

¿El usuario local también puede encender el vídeo?	No Después de que la consola local se desactive, el teclado y el mouse del usuario local se desactivarán y no podrán hacer cambios de configuración.
¿La desactivación del vídeo local también desactiva el teclado y el mouse locales?	Sí
¿La desactivación de la consola local desactivará el vídeo en la sesión de consola remota?	No, la activación o desactivación del vídeo local es independiente de la sesión de consola remota.
¿Cuáles son los privilegios necesarios para que un usuario de iDRAC active o desactive el vídeo del servidor local?	Cualquier usuario con privilegios de configuración del iDRAC 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 redirección de consola** de la interfaz web del iDRAC. El comando **racadm getconfig -g cfgRacTuning** de la CLI de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**. El estado también se muestra en la pantalla de OSCAR de iKVM. Cuando la consola local está activada, aparece un indicador de estado verde al lado del nombre del servidor. Cuando está desactivada, un punto amarillo indica que el iDRAC ha bloqueado la consola local.
No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.
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. Para obtener más información, consulte el apartado Cómo establecer la configuración regional en Linux.
¿Por qué aparece una pantalla en blanco en el servidor administrado al cargar el sistema operativo Windows 2000?	El servidor administrado no tiene el archivo controlador correcto de vídeo ATI. Deberá actualizar al archivo controlador de vídeo con el CD *Dell PowerEdge Installation and Server Management*.
¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la redirección de consola?	El BIOS de Dell emula el controlador de mouse como mouse PS/2. Debido al diseño, el mouse PS/2 usa la posición relativa para el apuntador de mouse, lo que ocasiona un retraso en la sincronización. El iDRAC tiene un controlador de mouse USB, que permite la posición absoluta y un seguimiento más preciso del apuntador del mouse. Aun cuando el iDRAC pasara la posición absoluta del mouse USB al BIOS de Dell, la emulación del BIOS lo convertiría nuevamente a la posición relativa y el comportamiento seguiría siendo el mismo. Para resolver este problema, defina el modo de mouse como **NINGUNO** en la configuración de redirección de consola.
¿Por qué no se sincroniza el mouse en la consola de texto de Linux?	El KVM virtual necesita 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 el mouse adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de redirección de consola. Compruebe que **Sincronizar el mouse** esté seleccionado en el menú **Mouse**. Presione <Alt><M> o seleccione **Mouse**→ **Sincronizar el mouse** para activar/desactivar la sincronización del mouse. Cuando la sincronización esté activada, aparecerá una marca junto a la selección en el menú **Mouse**.
¿Por qué no puedo usar un teclado o mouse mientras instalo un sistema operativo Microsoft® de manera remota por medio de la redirección de consola de iDRAC?	Cuando instala de manera remota un sistema operativo Microsoft admitido en un sistema con la redirección de consola habilitada en el BIOS, aparece un mensaje de conexión de EMS que le pide que seleccione **Aceptar** para poder continuar. Usted no puede usar el mouse para seleccionar **Aceptar** de manera remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la redirección de consola en el BIOS. Microsoft genera este mensaje para avisar al usuario que la redirección de consola está activada. Para asegurar que este mensaje no aparece, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Núm de mi estación de administración no muestra el estado de Bloq Núm en el servidor remoto?	Cuando se accede por medio de iDRAC, 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 Núm depende de la configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Núm en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una sesión de redirección de consola desde el host local?	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado ¿recibiré un mensaje de advertencia?	No Si un usuario local tiene acceso al sistema, tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?	Dell recomienda una conexión de 5 MB/s para un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la redirección de consola?	Se requiere que la estación de administración tenga un procesador Intel Pentium III a 500 MHz con al menos 256 MB de RAM.

Regresar a la página de contenido

Regresar a la página de contenido

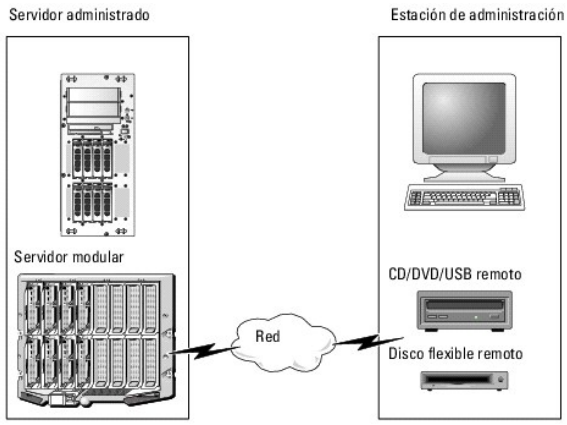
Configuración y uso de medios virtuales

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Información general

El componente **Medios virtuales**, que puede encontrar a través del visor de redirección de consola, permite que el servidor administrado tenga acceso a medios conectados a un sistema remoto en la red. La figura 9-1 muestra la arquitectura general de los **Medios virtuales**.

Figura 9-1. Arquitectura general de medios virtuales



Por medio de los **Medios virtuales**, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar archivos controladores o incluso instalar nuevos sistemas operativos de manera remota desde las unidades de CD/DVD y de disco virtuales.

NOTA: Los **medios virtuales** requieren una amplitud de banda de red mínima disponible de 128 Kbps.

Los **Medios virtuales** definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: un dispositivo de disco flexible y un dispositivo de disco óptico.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando los **Medios virtuales** se conectan, todas las solicitudes de acceso a la unidad virtual de CD o de disco flexible provenientes del servidor administrado son dirigidas a la estación de administración por la red. La conexión de los **Medios virtuales** tiene el mismo efecto que insertar discos en los dispositivos físicos. Cuando los medios virtuales no están conectados, los dispositivos virtuales en el servidor administrado se comportan como dos unidades sin discos insertados en ellas.

La tabla 9-1 lista las conexiones compatibles de unidades ópticas virtuales y de disco flexible virtuales.

NOTA: Si cambia los **medios virtuales** mientras están conectados podría detener la secuencia de inicio de sistema.

Tabla 9-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco flexible virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 pulgadas con disquete de 1,44 pulgadas	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disco flexible USB con un disquete de 1,44 pulgadas	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44 pulgadas	Unidad USB de CD-ROM con disco CD-ROM
Disco extraíble USB	

Estación de administración con Windows

Para ejecutar la función de **Medios virtuales** en una estación de administración que ejecuta el sistema operativo Microsoft® Windows®, instale una versión compatible de Internet Explorer con el complemento de control de ActiveX (consultar Exploradores web admitidos). Establezca la seguridad del explorador en el nivel **Medio** o en un nivel inferior para permitir que Internet Explorer descargue e instale los controles ActiveX firmados.

Dependiendo de su versión de Internet Explorer, es posible que se le solicite una configuración de seguridad personalizada para ActiveX:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Opciones de Internet** y después haga clic sobre la ficha **Seguridad**.
3. En **Seleccionar una zona de contenido web para especificar su configuración de seguridad**, haga clic para seleccionar la zona deseada.
4. En **Nivel de seguridad para esta zona,** haga clic en **Nivel personalizado**.

   Aparece la ventana **Configuración de seguridad.**
5. En **Controles y plug-ins ActiveX**, asegúrese de que las siguientes opciones estén fijadas en **Permitir**:
   - Permitir Scriptlets
   - Solicitud automática para controles de ActiveX
   - Descargar controles firmados de ActiveX
   - Descargar controles no firmados de ActiveX
6. Haga clic sobre **Aceptar** para guardar cualquier cambio y cierre la ventana de **Configuración de seguridad**.
7. Haga clic en **Aceptar** para cerrar la ventana de **Opciones de Internet Options**.
8. Reinicie Internet Explorer.

Se deben tener derechos de administrador para instalar ActiveX. Antes de instalar el control ActiveX, es posible que Internet Explorer muestre una advertencia de seguridad. Para completar el procedimiento de instalación del control ActiveX, acepte el control ActiveX cuando Internet Explorer muestre la advertencia de seguridad.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Firefox. Para obtener más información, consulte el apartado Exploradores web admitidos.

Se requiere Java Runtime Environment (JRE) para ejecutar el complemento de redirección de consola. Puede descargar JRE desde el sitio **java.sun.com**. Se recomienda la versión 1.6 o superiores de JRE.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz web del iDRAC.
2. Seleccione **Sistema** en el árbol de navegación y haga clic en la ficha **Consola**.
3. Haga clic en **Configuración**→ **Medios virtuales** para configurar los valores de los medios virtuales.

   La tabla 9-2 describe los valores de configuración de los **Medios virtuales**.
4. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 9-3.

Tabla 9-2. Valores de configuración de los medios virtuales

Atributo	Valor
Conectar medios virtuales	**Conectar**: conecta inmediatamente los **Medios virtuales** al servidor. **Desconectar**: desconecta inmediatamente los **Medios virtuales** del servidor. **Conectar automáticamente**: conecta los **Medios virtuales** al servidor únicamente cuando se inicia una sesión de medios virtuales.
Número máximo de sesiones	Muestra el número máximo de sesiones de **Medios virtuales** permitidas. Éste siempre es 1.
Sesiones activas	Muestra el número actual de sesiones de medios virtuales.
Cifrado activado para medios virtuales	Haga clic en la casilla de marcación para activar o desactivar el cifrado en conexiones de **Medios virtuales**. Si está seleccionado activa el cifrado; si no está seleccionado desactiva el cifrado.
Número de puerto de los medios virtuales	El número de puerto de red que se usa para conectarse al servicio de **Medios virtuales** sin cifrado. Dos puertos consecutivos a partir del número de puerto especificado se usan para conectar al servicio de **Medios virtuales**. El número de puerto después del puerto

	especificado no se debe configurar para ningún otro servicio del iDRAC. El valor predeterminado es **3668**.
Número de puerto SSL de los medios virtuales	El número de puerto de red utilizado para conexiones cifradas del servicio de **Medios virtuales**. Dos puertos consecutivos a partir del número de puerto especificado se usan para conectar al servicio de **Medios virtuales**. El número de puerto después del puerto especificado no se debe configurar para ningún otro servicio del iDRAC. El valor predeterminado es **3670**.
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** aparecerá como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB.
Activar el inicio una vez	Seleccione esta casilla para activar la opción para iniciar una vez. Esta opción automáticamente termina la sesión de **Medios virtuales** después de que el servidor se inicia una vez. Esta opción es útil para implementaciones automáticas.

Tabla 9-3. Botones de la página de configuración de medios virtuales

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de consola** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de consola**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la página **Configuración de consola**.

Ejecución de los medios virtuales

AVISO: 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.

AVISO: La aplicación Visor de consola debe permanecer activa mientras usted accede a los medios virtuales.

1. Abra un explorador de web compatible en la estación de administración. Consulte el apartado Exploradores web admitidos.
2. Inicie la interfaz web del iDRAC. Acceso a la interfaz web.
3. Seleccione **Sistema** en el árbol de navegación y haga clic en la ficha **Consola**.

   Aparecerá la página **Redirección de consola**. Si desea cambiar los valores de cualquiera de los atributos mostrados, consulte Configuración de los medios virtuales.

   NOTA: Es posible que aparezca **Archivo de imagen de disco flexible** bajo **Unidad de disco flexible** (si se aplica), pues este dispositivo se puede hacer un disco flexible virtual. Puede seleccionar una unidad óptica y un disco flexible al mismo tiempo o una sola unidad.

   NOTA: Las letras de unidad de los dispositivos virtuales en el servidor administrado no coinciden con las letras de unidades físicas en la estación de administración.

   NOTA: Es posible que los **medios virtuales** no funcionen correctamente en los clientes con sistema operativo Windows que estén configurados con seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador.

4. Haga clic en **Iniciar el visor**.

   NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo preguntará qué desea hacer con el archivo. Elija la opción de **Abrir con el programa** y después seleccione la aplicación **javaws**, que se encuentra en el subdirectorio **bin** del directorio de instalación de JRE.

   La aplicación **iDRACView** se ejecuta en una ventana por separado.

5. Haga clic en **Medios→ Asistente de medios virtuales...**.

   Aparecerá el asistente de redirección de medios.

6. Observe la ventana de estado. Si hay algún medio conectado, deberá desconectarlo antes de conectar otro medio. Haga clic en el botón **Desconectar** que se encuentra a la derecha del medio que desea desconectar.
7. Seleccione el botón de radio que está junto a los tipos de medios que desea conectar.

   Puede seleccionar un botón de radio en la sección **Unidad de USB/disco flexible** y uno en la sección **Unidad de CD/DVD**.

   Si desea conectar una imagen de disco flexible o una imagen ISO, introduzca la ruta de acceso (en el equipo local) de la imagen o haga clic en el botón **Examinar** y desplácese hacia a la imagen.

8. Haga clic en el botón **Conectar** que se encuentra junto a cada tipo de medio seleccionado.

   Los medios están conectados y la ventana de estado se actualiza.

9. Haga clic en el botón **Cerrar**.

Desconexión de los medios virtuales

1. Haga clic en **Medios→ Asistente de medios virtuales...**.
2. Haga clic en **Desconectar** junto al medio que desea desconectar.

   El medio se desconectará y se actualizará la ventana de estado.
3. Haga clic en **Close** (Cerrar).

Inicio desde los medios virtuales

El BIOS de sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disquete 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 el valor en el BIOS, realice los pasos a continuación:

1. Inicie el servidor administrado.
2. Presione <F2> para ingresar a la ventana de configuración del BIOS.
3. Desplácese a la secuencia de inicio y presione <Entrar>.

   En la ventana emergente, aparece una lista de las unidades virtuales ópticas y de disco flexible virtuales con otros dispositivos normales de inicio.
4. Asegúrese que la unidad virtual esté activada y que aparezca como el primer dispositivo con medio iniciable. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.
5. Guarde los cambios y salga.

   El servidor administrado se reinicia.

   El servidor administrado intenta iniciarse a partir de un dispositivo iniciable con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio iniciable está presente, el sistema se iniciará a partir del dispositivo virtual. De lo contrario, el sistema ignorará el dispositivo; como ocurriría con un dispositivo físico que no tiene medios iniciables.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas en terminar. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de los **Medios virtuales** puede tardar menos de 15 minutos en terminar. Para obtener más información, consulte el apartado Instalación del sistema operativo.

1. Verifique lo siguiente:
   - El CD de instalación de sistema operativo está insertado en la unidad de CD de la estación de administración.
   - La unidad de CD local está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección Inicio desde los medios virtuales para asegurarse que el BIOS está configurado para que inicie desde la unidad de CD a partir de la que se realiza la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

Uso de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En sistemas con Windows, las unidades de medios virtuales se montan automáticamente cuando están conectadas y se configuran con una letra de unidad.

El uso de las unidades virtuales desde el interior de Windows es similar al uso de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estarán disponibles en el sistema cuando se haga clic en la unidad y se examine el contenido de la misma.

Sistemas con Linux

En función de la configuración del software del sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, monte manualmente las unidades con el comando **mount** de Linux.

Preguntas más frecuentes

La tabla 9-4 contiene las preguntas y respuestas frecuentes.

Tabla 9-4. Uso de los medios virtuales: Preguntas frecuentes

Question	Answer
Algunas veces noto que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?	Cuando se agota el tiempo de espera de la red, el firmware de iDRAC abandona la conexión, desconectando 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 iDRAC 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 iDRAC?	Consulte Sistemas operativos admitidos para ver una lista de los sistemas operativos compatibles.
¿Qué exploradores web son compatibles con el iDRAC?	Consulte Exploradores web admitidos para ver una lista de los exploradores de web admitidos.
¿Por qué a veces se pierde mi conexión de cliente?	• Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD?en la unidad de CD del sistema cliente, en nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión cuando el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior. • Cuando se agota el tiempo de espera de la red, el firmware de iDRAC abandona la conexión, desconectando el vínculo entre el servidor y la unidad virtual. Asimismo, alguien puede haber cambiado los valores de configuración de los medios virtuales en la interfaz web o mediante comandos de RADACM. Para restablecer la conexión con el disco virtual, use la función de **Medios virtuales**.
La instalación del sistema operativo Windows parece tardar demasiado. ¿Por qué?	Si va a instalar el sistema operativo Windows con el CD *Dell PowerEdge Installation and Server Management* y una conexión de red lenta, el procedimiento de instalación puede requerir un tiempo prolongado para acceder a la interfaz web del iDRAC debido a la latencia de la red. Mientras la ventana de instalación no indique el progreso de la instalación, significa que el procedimiento de instalación está en progreso.
Veo el contenido de una unidad de disco flexible o memoria USB. Si trato de establecer una conexión de medios virtuales con la misma unidad, recibo un mensaje de error de conexión y se me pide que vuelva a intentarlo. ¿Por qué?	No se permite el acceso simultáneo a las unidades de disco flexible virtual. Cierre la aplicación que se usa para ver el contenido de la unidad antes de que intente hacer virtual la unidad.
¿Cómo configuro mi dispositivo virtual como dispositivo iniciable?	En el servidor administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Localice el CD virtual, el disco flexible virtual o la memoria flash virtual y cambie el orden de dispositivo de inicio según corresponda. Por ejemplo, para iniciar a partir de una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.
¿A partir de qué tipos de medios puedo iniciar el sistema?	El iDRAC permite iniciar a partir de los medios iniciables siguientes: • Medios de CDROM/DVD de datos • Imagen ISO 9660 • Imagen de disco flexible o disco flexible de 1,44 pulgadas • Una memoria USB a la que el sistema operativo reconoce como disco extraíble • Una imagen de memoria USB
¿Cómo puedo hacer que mi memoria USB sea iniciable?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para hacer que la memoria USB de Dell funcione como dispositivo de inicio. Usted puede iniciar también con un disco de arranque de Windows 98 y copiar los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, en la petición de DOS, escriba el comando siguiente: `sys a: x: /s` donde *x*: es la memoria USB que desea hacer iniciable. También puede usar la utilidad de inicio de Dell para crear una memoria USB iniciable. Esta utilidad sólo es compatible con las memorias USB de marca Dell. Para descargar la utilidad, abra un explorador de web, navegue al sitio web de asistencia Dell Support que se encuentra en **support.dell.com** y busque R122672.exe.
No puedo encontrar el dispositivo de disco flexible virtual en un sistema que ejecuta el sistema operativo Red Hat® Enterprise Linux® o SUSE® Linux. Mis medios virtuales están conectados y estoy conectado a mi disco flexible remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disco flexible 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 una petición de comandos de Linux y ejecute el siguiente comando: `grep "Disco flexible virtual" /var/log/messages` 2. Localice la última anotación de dicho mensaje y anote la hora. 3. En la petición 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 virtual Dell. 5. Asegúrese que está conectado a la unidad de disco flexible virtual. 6. En la petición de comandos de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
¿Qué tipo de sistemas de archivos son compatibles con mi unidad de disco virtual?	Su unidad de disco virtual es compatible con sistemas de archivos FAT16 o FAT32.
Cuando ejecuté una actualización de firmware de manera remota por medio de la interfaz web de iDRAC, mis unidades virtuales en el servidor se desmontaron. ¿Por qué?	Las actualizaciones de firmware hacen que el iDRAC se restablezca, que abandone la conexión remota y que desmonte las unidades virtuales. Las unidades volverán a aparecer cuando el restablecimiento del iDRAC termine.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de RACADM local

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

La interfaz de línea de comando (CLI) de RACADM local brinda acceso a las funciones de administración del iDRAC desde el servidor administrado. RACADM brinda acceso a las mismas funciones que la interfaz web del iDRAC. Sin embargo, RACADM se puede usar con secuencias de comandos para facilitar la configuración de varios servidores y controladores iDRAC, mientras que la interfaz web es más útil para la administración interactiva.

Los comandos de RACADM local no usan las conexiones de red para acceder al iDRAC desde el servidor administrado. Esto significa que usted puede usar comandos de RACADM local para configurar el sistema inicial de red del iDRAC.

Para obtener más información sobre cómo configurar varios iDRAC, consulte Configuración de varios iDRAC.

Esta sección ofrece la siguiente información:

- Uso de RACADM desde una petición de comandos
- Configuración de iDRAC por medio del comando **racadm**
- Uso del archivo de configuración de RACADM para configurar varios iDRAC

Uso del comando RACADM

Los comandos de RACADM se ejecutan de manera local (en el servidor administrado) desde una petición de comandos o petición de shell.

Inicie sesión en el servidor administrado, abra un shell de comandos e introduzca comandos de RACADM local en el formato siguiente:

```
racadm <subcomando> -g <grupo> -o <objeto> <valor>
```

Sin opciones, el comando RACADM muestra la información general de uso. Para mostrar la lista de subcomandos de RACADM, escriba:

```
racadm help
```

La lista de subcomandos incluye todos los comandos compatibles con el iDRAC.

Para obtener ayuda para un subcomando, escriba:

```
racadm help <subcomando>
```

El comando muestra la sintaxis y las opciones de línea de comandos del subcomando.

Subcomandos de RACADM

Tabla 10-1 proporciona una descripción de cada uno de los subcomandos de RACADM que se pueden ejecutar en RACADM. Para ver una lista detallada de los subcomandos de RACADM que incluye la sintaxis y las anotaciones válidas, consulte Generalidades del subcomando RACADM.

Tabla 10-1. Subcomandos de RACADM

Comando	Descripción
clrraclog	Borra el registro de iDRAC. Después de borrarlo, sólo se hace una anotación para indicar el usuario que borró el registro y la hora en la que se borró.
clrsel	Borra las anotaciones del registro de sucesos del sistema del servidor administrado.
config	Configura el iDRAC.
getconfig	Muestra las propiedades de configuración actuales del iDRAC.
getniccfg	Muestra la configuración IP actual del controlador.
getraclog	Muestra el registro de iDRAC.
getractime	Muestra la hora del iDRAC.
getssninfo	Muestra información sobre las sesiones activas.
getsvctag	Muestra las etiquetas de servicio.
getsysinfo	Muestra información sobre el iDRAC y el servidor administrado, incluyendo la configuración de IP, el modelo de hardware, las versiones de firmware y la información del sistema operativo.
gettracelog	Muestra el registro de rastreo de iDRAC. Si se usa con -i, el comando muestra el número de anotaciones en el registro de rastreo de

	iDRAC.
help	Muestra una lista de subcomandos del iDRAC.
help <*subcomando*>	Muestra la descripción de uso del subcomando especificado.
racreset	Restablece el iDRAC.
racresetcfg	Restablece la configuración predeterminada del iDRAC.
serveraction	Realiza operaciones de administración de alimentación en el servidor administrado.
setniccfg	Establece la configuración IP para el controlador.
sslcertdownload	Descarga un certificado de CA.
sslcertupload	Carga un certificado de CA o un certificado de servidor en el iDRAC.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el iDRAC.
sslcsrgen	Genera y descarga la CSR de SSL.
testemail	Obliga al iDRAC a enviar un correo electrónico a través del NIC de iDRAC.
testtrap	Obliga al iDRAC a enviar una alerta SNMP a través del NIC de iDRAC.

Uso de la utilidad RACADM para configurar el iDRAC

Esta sección describe cómo usar RACADM para realizar varias tareas de configuración del iDRAC.

Cómo mostrar la configuración actual del iDRAC

El subcomando **getconfig** de RACADM obtiene los valores de configuración actuales del iDRAC. Los valores de configuración se organizan en *grupos* que contienen uno o varios *objetos* y los objetos tienen *valores*.

Consulte Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC para ver una descripción completa de los grupos y objetos.

Para mostrar una lista de todos los grupos de iDRAC, introduzca este comando:

```
racadm getconfig -h
```

Para mostrar los objetos y valores de un grupo en particular, introduzca este comando:

```
racadm getconfig -g <grupo>
```

Por ejemplo, para mostrar una lista de todos los valores del objeto de grupo **cfgLanNetworking**, escriba el comando siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Administración de usuarios del iDRAC con RACADM

AVISO: Tenga precaución cuando utilice el comando **racresetcfg**, pues se restablecerán *todos* los parámetros de configuración predeterminados originales. Todos los cambios anteriores se perderán.

NOTA: Si está configurando un iDRAC nuevo o si ha ejecutado el comando **racadm racresetcfg**, el único usuario actual es **root** con la contraseña **calvin**.

NOTA: Los usuarios pueden activarse o desactivarse posteriormente. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC.

Puede configurar hasta 15 usuarios en la base de datos de propiedades de iDRAC. El decimosexto usuario se reserva para el usuario de LAN de IPMI. Antes de activar manualmente un usuario de iDRAC, verifique si existe algún usuario actual.

Para verificar si existe un usuario, escriba el comando siguiente en la petición de comandos:

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

O bien:

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

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

NOTA: También puede escribir racadm getconfig -f <*nombre_de_archivo*> y ver el archivo <*nombre-_de_archivo*> que se genera y que incluye a todos los usuarios, así como todos los demás parámetros de configuración del iDRAC.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=nn

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 =, significa que ese índice está asignado a ese nombre de usuario.

Cómo agregar un usuario de iDRAC

Para agregar un nuevo usuario al iDRAC, realice los pasos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca el privilegio de inicio de sesión en el iDRAC para el usuario.
4. Active el usuario.

Ejemplo

El ejemplo a continuación describe cómo agregar un nuevo usuario de nombre "Juan" con una contraseña "123456" y privilegios de inicio de sesión en el iDRAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

Para verificar el usuario nuevo, use uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig -g cfgUserAdmin -i 2
```

Activación de un usuario del iDRAC con permisos

Para otorgar permisos administrativos específicos (en base a funciones) a un usuario, configure la propiedad **cfgUserAdminPrivilege** con una máscara de bits creada a partir de los valores que se muestran en tabla 10-2:

Tabla 10-2. Máscaras de bit para privilegios del usuario

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

Por ejemplo, para permitir al usuario **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros** y **Acceder a la redirección de consola**, agregue los valores 0x00000002, 0x00000004, 0x00000008 y 0x00000010 para crear el mapa de bits 0x0000002E. Después introduzca el siguiente comando para establecer el privilegio:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

Cómo eliminar un usuario de iDRAC

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

El ejemplo siguiente ilustra la sintaxis de comando que se puede usar para eliminar un usuario de RAC:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <índice> &amp;quot;&amp;quot;
```

Una cadena nula de dos caracteres de comillas ("") indica al iDRAC que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.

Pruebas de las alertas por correo electrónico

La función de alertas por correo electrónico del iDRAC permite a los usuarios recibir alertas por correo electrónico cuando se produce un suceso crítico en el servidor administrado. El siguiente ejemplo muestra cómo probar la función de alertas por correo electrónico para asegurarse de que el iDRAC pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Asegúrese de que los valores de SMTP y de alerta por correo electrónico estén configurados antes de probar la función de alertas por correo electrónico. Para obtener más información, consulte Configuración de alertas por correo electrónico.

Cómo probar la función de alertas de capturas SNMP del iDRAC

La función de envío de alertas de capturas SNMP del iDRAC permite que las configuraciones de oyentes de capturas SNMP reciban capturas de los sucesos de sistema que se presentan en el servidor administrado.

El ejemplo a continuación muestra cómo un usuario puede probar la función de alertas de capturas SNMP.

```
racadm testtrap -i 2
```

NOTA: Antes de probar la función de alertas de capturas SNMP del iDRAC, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Consulte las descripciones de lo subcomandos **testtrap** y **testemail** para configurar estos valores.

Configuración de las propiedades de red del iDRAC

Para generar una lista de las propiedades disponibles de red, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Para utilizar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** y active esta función:

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

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración de iDRAC cuando se le pide que pulse <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC, consulte LAN.

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de red LAN deseadas.

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN de iDRAC se desactivará aun cuando DHCP esté activado.

Configuración de IPMI

1. Configure la IPMI en la LAN con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

   a. Actualice los privilegios de canal de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>
```

donde <*nivel*> es uno de los siguientes valores:

- 2 (**Usuario**)
- 3 (**Operador**)
- 4 (**Administrador**)

Por ejemplo, para definir el privilegio de canal de LAN de IPMI en 2 (usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

b. De ser necesario, defina la clave de cifrado del canal de la LAN de IPMI con un comando como el siguiente:

NOTA: La IPMI de iDRAC es compatible con el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>
```

donde <*clave*> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

2. Configure la comunicación en serie en la LAN (SOL) con el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

NOTA: El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación IPMI 2.0.

a. Actualice el nivel mínimo de privilegio de la SOL de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>
```

donde <*nivel*> es uno de los siguientes:

- 2 (**Usuario**)
- 3 (**Operador**)
- 4 (**Administrador**)

Por ejemplo, para definir los privilegios de IPMI como 2 (Usuario), introduzca el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

NOTA: Para redirigir la consola de 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.

b. Actualice la velocidad en baudios de la SOL de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_en_baudios>
```

donde <*velocidad_en_baudios*> es 19200, 57600 o 115200 bps.

Por ejemplo:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Active la comunicación en serie en la LAN escribiendo el comando siguiente en la petición de comandos.

NOTA: Cada usuario individual puede activar o desactivar la SOL.

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <identificación> 2
```

donde <*identificación*> es la identificación única del usuario.

Configuración del PEF

Puede configurar la acción que desea que el iDRAC ejecute ante cada alerta de plataforma. Tabla 10-3 muestra las acciones posibles y el valor para identificarlas en RACADM.

Tabla 10-3. Acción de sucesos de plataforma

Acción	Valor
Sin acción	0

Apagado	1
Reiniciar	2
Ciclo de encendido	3

1. Configure acciones de filtro de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <índice> <valor_de_acción>
   ```

   donde <*índice*> es el índice de filtro de sucesos de plataforma (consulte la tabla 5-6) y <*valor_de_acción*> es un valor de tabla 10-3.

   Por ejemplo, para hacer que el filtro de sucesos de plataforma reinicie el sistema y envíe una alerta de IPMI cuando se detecte un suceso crítico del procesador, escriba el siguiente comando:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
   ```

Configuración de la PET

1. Active las alertas globales con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active la captura de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <índice> <0|1>
   ```

   donde <*índice*> es el índice de destino de la captura de sucesos de plataforma y `0` o `1` desactiva o activa la captura de sucesos de plataforma, respectivamente.

   Por ejemplo, para activar una PET con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

3. Configure la política de captura de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <índice> <dirección_IP>
   ```

   donde *índice* es el índice del destino de la captura de sucesos de plataforma y <*dirección_IP*> es la dirección 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>
   ```

   donde <*nombre*> es el nombre de comunidad de la captura de sucesos de plataforma.

Configuración de alertas por correo electrónico

1. Active las alertas globales con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico con los comandos siguientes:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <índice> <0|1>
   ```

   donde <*índice*> es el índice del destino de correo electrónico y 0 desactiva la alerta por correo electrónico o 1 activa la alerta. El índice de destino de correo electrónico puede ser un valor de 1 a 4.

   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 de correo electrónico con el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>
   ```

   donde 1 es el índice del destino del mensaje de correo electrónico y <*dirección_de_correo_electrónico*> es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

4. Para configurar un mensaje personalizado, introduzca el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <índice> <mensaje_personalizado>
   ```

   donde *índice* es el índice del destino del mensaje de correo electrónico y <*mensaje_personalizado*> es el mensaje personalizado.

5. Si lo desea, pruebe la alerta configurada de correo electrónico con el comando siguiente:

   ```
   racadm testemail -i <índice>
   ```

   donde <*índice*> es el índice del destino de correo electrónico que va a probar.

Configuración de la filtración de IP (IpRange)

La filtración de direcciones IP (o *Comprobación de rango de IP*) permite el acceso al iDRAC únicamente a los clientes o estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Todas las demás solicitudes de inicio de sesión son denegadas.

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 las direcciones IP entrantes y a las propiedades de **cfgRacTuneIpRangeAddr**. Si los resultados son idénticos, se permite que la petición de inicio de sesión entrante tenga acceso al iDRAC. Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión procederá si el valor de la siguiente expresión es igual a cero:

```
cfgRacTuneIpRangeMask & (<dirección_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

donde & es el operador Y a nivel de bits de las cantidades y ^ es el operador O exclusivo a nivel de bits.

Consulte cfgRacTuning para ver una lista completa de las propiedades de **cfgRacTuning**.

Tabla 10-4. 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 se basa en el modo en bits y *AND* con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. Se permite que cualquier dirección IP que contenga este patrón de bits en los bits superiores inicie sesión. Los inicios de sesión que provengan de las direcciones de IP estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que el rango de direcciones de 192.168.1.0 a 192.168.1.255 inicien sesión.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara debe darse en forma de máscara de red, donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior.

Configuración de la filtración de IP

Para configurar la filtración de IP en la interfaz web, siga estos pasos:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red / Seguridad**.
2. En la página **Configuración de red**, haga clic en **Configuración avanzada**.
3. Marque la casilla **Rango IP activado** e introduzca la **Dirección de rango IP** y la **Máscara de subred de rango IP**.
4. Haga clic en **Aplicar**.

A continuación se presentan ejemplos de cómo usar RACADM local para configurar la filtración de IP.

NOTA: Consulte Uso de la interfaz de línea de comandos de RACADM local para obtener más información sobre RACADM y los comandos RACADM.

1. Los siguientes comandos RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57:

   ```
   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
   ```

2. Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

El último byte de la máscara de rango está establecido como 252, el equivalente decimal de 11111100b.

Directrices para el filtrado de IP

Utilice las directrices a continuación cuando active el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Use la dirección base del rango deseado 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.

Configuración del 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 iDRAC durante un lapso de tiempo predefinido.

Las funciones del bloqueo de IP incluye:

- El número de fallas permitidas de inicio de sesión (**cfgRacTuneIpBlkFailcount**)
- El periodo en segundos durante el cual se deben presentar estas fallas (**cfgRacTuneIpBlkFailWindow**)
- La cantidad de tiempo en segundos durante el que se impide que la dirección IP bloqueada establezca una sesión después de haber excedido el número de fallas permitidas (**cfgRacTuneIpBlkPenaltyTime**)

Conforme se acumulan las fallas de inicio de sesión provenientes de una dirección IP específica, un contador interno lleva registro de las mismas. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: Identificación de intercambio de SSH: el host remoto ha cerrado la conexión.

Consulte Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC para ver una lista completa de las propiedades de **cfgRacTune**.

Propiedades de restricción de reintentos de inicio de sesión muestra una lista de los parámetros definidos por el usuario.

Tabla 10-5. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presenten fallas consecutivas (**cfgRacTuneIpBlkFailCount**) provenientes de una única dirección IP dentro de lapso de tiempo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecimiento de sesión que provengan de dicha dirección serán rechazados durante un período de tiempo determinado (**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 periodo en segundos durante el cual se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.
cfgRacTuneIpBlkPenaltyTime	Define el período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas.

Activación del bloqueo de IP

El ejemplo siguiente impide a una dirección IP cliente establecer una sesión durante cinco minutos si dicho cliente ha fallado cinco intentos de inicio de sesión en un período de un minuto.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente evita más de tres intentos fallidos dentro de un minuto y evita los intentos de inicio adicionales durante una hora.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

Configuración de los servicios de Telnet y SSH del iDRAC por medio de RACADM local

La consola de Telnet/SSH se puede configurar de manera local (en el servidor administrado) con los comandos de RACADM.

NOTA: Se debe tener permiso de **Configurar el iDRAC** para ejecutar los comandos en esta sección.

NOTA: Cuando usted reconfigura los valores de Telnet o SSH en el iDRAC, todas las sesiones actuales se terminan sin advertencia.

Para activar Telnet y SSH desde RACADM local, inicie sesión en el servidor administrado y escriba los siguientes comandos en el símbolo de sistema:

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

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

Para desactivar el servicio Telnet o SSH, cambie el valor de `1` a `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0

racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Escriba el siguiente comando para cambiar el número de puerto de Telnet en el iDRAC:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <número del nuevo puerto>
```

Por ejemplo, para cambiar el puerto Telnet del valor predeterminado 22 a 8022, escriba este comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Para ver una lista completa de los comandos disponibles de la CLI de RACADM, consulte Uso de la interfaz de línea de comandos de RACADM local.

Uso de un archivo de configuración de iDRAC

El archivo de configuración de iDRAC es un archivo de texto que contiene una representación de los valores en la base de datos de iDRAC. Puede usar el subcomando **getconfig** de RACADM para generar un archivo de configuración que contenga los valores actuales del iDRAC. Puede modificar entonces el archivo y usar el subcomando **config -f** de RACADM para cargar el archivo nuevamente en el iDRAC o para copiar la configuración a otros iDRAC.

Creación de un archivo de configuración de iDRAC

El archivo de configuración es un archivo de texto simple (sin formatos). Se puede usar cualquier nombre de archivo válido; la convención recomendada es la extensión de archivo **.cfg**.

El archivo de configuración se puede:

- Crear con un editor de textos
- Obtenerse del iDRAC con el subcomando **getconfig** de RACADM
- Obtenerse del iDRAC con el subcomando **getconfig** de RACADM y después editarse

Para obtener un archivo de configuración, con el comando **getconfig** de RACADM, introduzca el comando siguiente en la petición de comandos del servidor administrado:

```
racadm getconfig -f myconfig.cfg
```

Este comando crea el archivo **myconfig.cfg** en el directorio actual.

Sintaxis del archivo de configuración

AVISO: Modifique el archivo de configuración con un editor de textos sin formato, como el **Bloc de notas** en Windows o **vi** en Linux. La utilidad **racadm** analiza únicamente el texto ASCII. Los formatos confunden al analizador y pueden dañar la base de datos de iDRAC.

Esta sección describe el formato del archivo de configuración.

- Las líneas que comienzan con # son comentarios.

Un comentario *debe* comenzar en la primera columna de la línea. Un carácter # que esté en cualquier otra columna será tratado como carácter # normal.

Ejemplo:

```
#

# Esto es un comentario

[cfgUserAdmin]

cfgUserAdminPrivilege=4
```

- Todas las anotaciones de grupo deben estar encerradas en los caracteres ***[*** y ***]***.

El carácter inicial ***[*** que denota un nombre de grupo *debe* iniciar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC.

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 se especifican como pares *objeto=valor* sin espacio en blanco entre el objeto, el signo "=" y el valor.

El espacio en blanco que se incluye después del valor se ignora. El espacio en blanco dentro de una cadena de valores no se modifica. Todo carácter a la derecha del signo = se toma tal cual es (por ejemplo, un segundo = o un #, *[*, *]*, etc.).

- El analizador ignora una anotación de objeto de índice.

El usuario *no puede* especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva anotación en el primer índice disponible de dicho grupo.

El comando `racadm getconfig -f <nombre_de_archivo>` coloca un comentario frente a los objetos del índice, lo que permite ver los comentarios que se incluyen.

NOTA: Usted puede crear un grupo indexado manualmente con el siguiente comando: racadm config -g <*nombre_de_grupo*> -o <*objeto anclado*> -i <*índice*> <*nombre-de-ancla-único*>

- La línea para un grupo indexado *no se puede borrar* de un archivo de configuración.

El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

```
racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> -i <índice> &amp;quot;&amp;quot;
```

NOTA: Una cadena NULA (que se identifica por dos caracteres "") indica al iDRAC que elimine el índice del grupo especificado.

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

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

- Para grupos indexados, el ancla de objeto *debe ser* el primer objeto después del par *[ ]*. Los siguientes son ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]

cfgUserAdminUserName=<nombre_de_usuario>
```

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

El analizador lee en todos los índices de iDRAC para ese grupo. Los objetos dentro de dicho grupo son modificaciones simples cuando se configura el iDRAC. Si un objeto modificado representa un índice nuevo, el índice se crea en el iDRAC durante la configuración.

- No se puede especificar un índice deseado en un archivo de configuración.

Los índices se pueden crear y eliminar, por lo que con paso del tiempo, el grupo puede fragmentarse con índices usados y no usados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método permite flexibilidad al momento de agregar anotaciones indexadas en las que usted no necesita hacer coincidencias exactas de índice entre todos los RAC que se administran. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo de configuración que se analiza y se ejecuta correctamente en un iDRAC no funcione correctamente en otro si todos los índices están llenos y usted tiene que agregar un nuevo usuario.

Modificación de la dirección IP del iDRAC en un archivo de configuración

Cuando modifique la dirección IP de iDRAC en el archivo de configuración, elimine todas las anotaciones **<***variable***>**=<*valor*> innecesarias. Sólo la etiqueta variable real del grupo con "[" y "]" permanecerá, incluyendo las dos anotaciones **<***variable***>**=<*valor*> relacionadas con el cambio de la dirección IP.

Por ejemplo:

```
#
```

```
# Grupo de objeto &quot;cfgLanNetworking&quot;

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo se actualizará de la siguiente manera:

```
#

# Grupo de objeto &quot;cfgLanNetworking&quot;

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comentario, el resto de esta línea se ignora

cfgNicGateway=10.35.9.1
```

Carga del archivo de configuración en el iDRAC

El comando `racadm config -f <nombre_de_archivo>` analiza el archivo de configuración para verificar que el grupo y los nombres de objeto válidos estén presentes y que se cumpla con las reglas de la sintaxis. Si el archivo no tiene errores, el comando actualizará la base de datos del iDRAC con el contenido del archivo.

NOTA: Para verificar únicamente la sintaxis y no actualizar la base de datos del iDRAC, agregue la opción **-c** al subcomando **config**.

Los errores dentro del archivo de configuración se señalan con el número de línea y un mensaje que explica el problema. Usted deberá corregir todos los errores antes de que el archivo de configuración se pueda actualizar en el iDRAC.

AVISO: Use el subcomando **racresetcfg** para restablecer la base de datos y la configuración predeterminada original de la tarjeta de interfaz de red de iDRAC y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Antes ejecutar el comando `racadm config -f <nombre_de_archivo>`, puede ejecutar el subcomando **racreset** para restablecer la configuración predeterminada del iDRAC. Asegúrese de que el archivo que se va a cargar incluya todos los objetos, usuarios, índices y otros parámetros deseados.

Para actualizar el iDRAC con el archivo de configuración, ejecute el comando siguiente en la petición de comandos del servidor administrado:

```
racadm config -f <nombre_de_archivo>
```

Después de que el comando ha terminado, usted puede ejecutar el subcomando **getconfig** de RACADM para confirmar que la actualización fue satisfactoria.

Configuración de varios iDRAC

A través de un archivo de configuración, usted puede configurar otros iDRAC con propiedades idénticas. Siga estos pasos para configurar varios iDRAC:

1. Cree el archivo de configuración del iDRAC cuyos valores desea copiar en los demás. En una petición de comandos del servidor administrado, introduzca el comando siguiente:

   ```
   racadm getconfig -f <nombre_de_archivo>
   ```

   donde `<nombre_de_archivo>` es el nombre de un archivo para guardar las propiedades del iDRAC, como **myconfig.cfg**.

   Para obtener más información, consulte el Creación de un archivo de configuración de iDRAC.

   NOTA: Algunos archivos de configuración contienen información exclusiva de iDRAC (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros iDRAC.

2. Modifique el archivo de configuración que ha creado en el paso anterior y quite o marque como comentarios los valores que *no desea* reproducir.
3. Copie el archivo de configuración modificado en una unidad de red donde esté disponible para cada servidor administrado cuyo iDRAC desea configurar.
4. Para cada iDRAC que desea configurar:
   a. Inicie sesión en el servidor administrado y abra una petición de comandos.
   b. Si desea cambiar la configuración predeterminada del iDRAC, introduzca el comando siguiente:

```
racadm racreset
```

c. Cargue el archivo de configuración en el iDRAC con el comando siguiente:

```
racadm config -f <nombre_de_archivo>
```

donde <*nombre_de_archivo*> es el nombre del archivo de configuración que ha creado. Incluya la ruta de acceso completa si el archivo no está en el directorio de trabajo.

d. Restablezca el iDRAC que se configuró por medio del comando siguiente:

```
racadm reset
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de SM-CLP de iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Esta sección ofrece información acerca del Protocolo de línea de comandos de administración de servidor (SM-CLP) del Grupo de trabajo de administración de servidor (SMWG) que está incorporado en el iDRAC.

NOTA: Esta sección supone que el lector está familiarizado con la iniciativa SMASH (Arquitectura de administración de sistemas para hardware de servidor) y las especificaciones de SM-CLP de SMWG. Para obtener más información sobre estas especificaciones, visite el sitio web de DMTF (Grupo de trabajo de administración distribuida) en **www.dmtf.org**.

El SM-CLP de iDRAC es un protocolo impulsado por el DMTF y el SMWG para proporcionar estándares para las implementaciones de interfaz de línea de comandos para administración de sistemas. Se están realizando muchos esfuerzos para obtener una arquitectura SMASH definida como punto de partida para un conjunto de componentes de administración de sistemas más estandarizado. El SM-CLP de SMWG es un subcomponente de los esfuerzos generales de SMASH realizados por DMTF.

El SM-CLP ofrece un subconjunto de funciones de la interfaz de línea de comandos de RACADM local, pero con una ruta de acceso distinta. SM-CLP se ejecuta dentro del iDRAC, mientras que RACADM se ejecuta en el servidor administrado. Asimismo, RACADM es una interfaz patentada de Dell; SM-CLP es una interfaz estándar de la industria. Consulte Equivalencias de RACADM y SM-CLP para ver una relación de los comandos RACADM y SM-CLP.

Administración del sistema con SM-CLP

El SM-CLP del iDRAC permite administrar las siguientes funciones del sistema desde una línea de comandos o secuencia de comandos:

- Administración de la alimentación de servidor: enciende, apaga o reinicia el sistema
- Administración de registro de sucesos del sistema: muestra o borra las anotaciones del registro de sucesos del sistema
- Administración de cuentas de usuario del iDRAC
- Configuración de Active Directory
- Configuración de la LAN de iDRAC
- Generación de solicitudes de firma de certificados (CSR) de SSL
- Configuración de los medios virtuales
- Redirección de la comunicación en serie en la LAN (SOL) por medio de Telnet o SSH

Compatibilidad con SM-CLP de iDRAC

SM-CLP se aloja en el firmware del iDRAC y es compatible con conexiones de Telnet y SSH. La interfaz de SM-CLP de iDRAC está basada en la versión 1.0 de la especificación SM-CLP proporcionada por la organización DMTF.

Las siguientes secciones proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC.

Funciones de SM-CLP

La especificación SM-CLP proporciona un conjunto común de verbos estándares de SM-CLP que se pueden usar para la administración simple de sistemas por medio de la CLI.

El SM-CLP promueve el concepto de verbos y destinos para ofrecer capacidades de configuración de sistemas por medio de la CLI. El verbo indica la operación a realizar y el destino determina la entidad (u objeto) que ejecuta la operación.

A continuación se presenta la sintaxis de la línea de comandos de SM-CLP:

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

Tabla 11-1 muestra una lista de los verbos compatibles con la CLI del iDRAC, la sintaxis de cada comando y una lista de las opciones compatibles con los verbos.

Tabla 11-1. Verbos compatibles con la CLI de SM-CLP

Verbo	Descripción	Opciones
cd	Navega por el espacio de direcciones de sistema administrado por medio del shell. Sintaxis: cd [*opciones*] [*destino*]	-default, -examine, -help, -output, -version
delete	Elimina un objeto. Sintaxis: delete [*opciones*] *destino*	-examine, -help, -output, -version
dump	Lleva una imagen binaria del punto de acceso de administrabilidad a un URI. dump -destination <*URI*> [*opciones*] [*destino*]	-destination, -examine, -help, -output, -version
exit	Cierra la sesión de shell de SM-CLP. Sintaxis: exit [*opciones*]	-help, -output, -version
help	Muestra la ayuda de los comandos de SM-CLP. help	-examine, -help, -output, -version
load	Lleva una imagen binaria de un URI al punto de acceso de administrabilidad. Sintaxis: load -source <*URI*> [*opciones*] [*destino*]	-examine, -help, -output, -source, -version
reset	Restablece el destino. Sintaxis: reset [*opciones*] [*destino*]	-examine, -help, -output, -version
set	Establece las propiedades de un destino Sintaxis: set [*opciones*] [*destino*] <*nombre de propiedad*>=<*valor*>	-examine, -help, -output, -version
show	Muestra las propiedades, verbos y destinos secundarios del destino. Sintaxis: show [*opciones*] [*destino*] <*nombre de propiedad*>=<*valor*>	-all, -default, -display, -examine, -help, -level, -output, -version
start	Inicia un destino. Sintaxis: start [*opciones*] [*destino*]	-examine, -force, -help, -output, -version
stop	Desactiva un destino. Sintaxis: stop [*opciones*] [*destino*]	-examine, -force, -help, -output, -state, -version, -wait
version	Muestra los atributos de versión de un destino. Sintaxis: version [*opciones*]	-examine, -help, -output, -version

Tabla 11-2 describe las opciones de SM-CLP. Algunas opciones tienen formas abreviadas, según se muestra en la tabla.

Tabla 11-2. Opciones admitidas por CM-CLP

Opción de SM-CLP	Descripción
-all, -a	Indica al verbo que realice todas las funciones posibles.
-destination	Especifica la ubicación para guardar una imagen en el comando dump. Sintaxis: -destination <URI>
-display, -d	Filtra la salida generada por el comando. Sintaxis: -display <propiedades | destinos | verbos>[, <propiedades | destinos | verbos>]*

-examine, -x	Indica al procesador de comandos que valide la sintaxis del comando sin ejecutarlo.
-help, -h	Muestra la ayuda del verbo.
-level, -l	Indica al verbo que se aplique a destinos en niveles adicionales por debajo del destino especificado. Sintaxis: `-level <n | all>`
-output, -o	Especifica el formato de la salida. Sintaxis: `-output <text | clpcsv | clpxml>`
-source	Especifica la ubicación de una imagen en un comando de carga. Sintaxis: -source <URI>
-version, -v	Muestra el número de versión de SMASH-CLP.

Navegación del espacio de direcciones de MAP

NOTA: La diagonal (/) y la diagonal invertida (\) pueden intercambiarse en las rutas de acceso de direcciones en SM-CLP. Sin embargo, una diagonal invertida al final de una línea de comandos hace que el comando continúe en la línea siguiente y se ignora cuando el comando se ejecuta.

Los objetos que pueden ser administrados con SM-CLP se representan con destinos organizados en un espacio jerárquico denominado espacio de direcciones de Punto de acceso de administrabilidad (MAP). La ruta de acceso de la dirección especifica la ruta de acceso desde la raíz del espacio de direcciones hacia un objeto en el espacio de direcciones.

El destino raíz se representa con una diagonal (/) o una diagonal invertida (\). Es el punto de partida predeterminado cuando se inicia sesión en el iDRAC. Vaya hacia la raíz con el verbo cd. Por ejemplo, para navegar a la tercera anotación en el Registro de sucesos del sistema (SEL), introduzca el comando siguiente:

```
->cd /system1/sp1/logs1/record3
```

Introduzca el verbo cd sin destino para encontrar la ubicación actual en el espacio de direcciones. Las abreviaturas `..` y `.` funcionan de la misma forma que en Windows y Linux: `..` se refiere al nivel superior inmediato y `.` se refiere al nivel actual.

Destinos

tabla 11-3 muestra una lista de destinos disponibles por medio de SM-CLP.

Tabla 11-3. Destinos de SM-CLP

Destino	Definición
/system1/	El destino de sistema administrado.
/system1/sp1	El procesador de servicio.
/system1/sol1	Destino de la comunicación en serie en la LAN.
/system1/sp1/account1 a /system1/sp1/account16	Las dieciséis cuentas locales de usuario de iDRAC. account1 es la cuenta raíz.
/system1/sp1/enetport1	La dirección MAC del NIC del iDRAC.
/system1/sp1/enetport1/lanendpt1/ipendpt1	Los valores de la IP, puerta de enlace y máscara de red del iDRAC.
/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	La configuración del servidor DNS del iDRAC.
/system1/sp1/group1 a /system1/sp1/group5	Los grupos de esquema estándar de Active Directory.
/system1/sp1/logs1	El destino de la recolecciones de registro.
/system1/sp1/logs1/record1	Una anotación individual del registro de sucesos de sistema en el sistema administrado.
/system1/sp1/logs1/records	El destino del SEL en el sistema administrado.
/system1/sp1/oemdell_racsecurity1	El almacenamiento para los parámetros que se usan para generar una solicitud de firma de certificado.
/system1/sp1/oemdell_ssl1	El estado de la solicitud de certificado de SSL.
/system1/sp1/oemdell_vmservice1	La configuración y estado de los medios virtuales.

Uso del verbo show

Para conocer más sobre un destino, utilice el verbo show. Este verbo muestra las propiedades del destino, subdestinos y una lista de los verbos de SM-CLP que se permiten en la ubicación.

Uso de la opción -display

La opción **show -display** permite limitar la salida del comando de manera que muestre una o más propiedades, destinos y verbos. Por ejemplo, para mostrar sólo las propiedades y destinos en la ubicación actual, use el comando siguiente:

```
show -d properties,targets /system1/sp1/account1
```

Para mostrar únicamente ciertas propiedades, indíquelas, según se muestra en el comando siguiente:

```
show -d properties=(userid,username) /system1/sp1/account1
```

Si sólo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción -level

La opción **show -level** ejecuta **show** en más niveles dentro del destino especificado. Por ejemplo, si desea consultar las propiedades **username** y **userid** de los destinos **account1** a **account16** bajo **/system1/sp1**, puede introducir el comando siguiente:

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

Para consultar todos los destinos y propiedades en el espacio de direcciones, utilice la opción **-l all**, como se indica en el comando siguiente:

```
show -l all -d properties /
```

Uso de la opción -output

La opción **-output** especifica uno de cuatro formatos para la salida de los verbos de SM-CLP: **text**, **clpcsv**, **keyword** y **clpxml**.

El formato predeterminado es **text** y es el mensaje de salida más legible. El formato **clpcsv** es un formato de valores separados con comas que es apto para cargar un programa de hoja de cálculo. El formato **keyword** muestra la información a manera de lista de pares palabra_clave=valor, un par por línea. El formato **clpxml** es un documento XML que contiene el elemento XML **response**. DMTF creó especificaciones para los formatos **clpcsv** y **clpxml**, que se encuentran en el sitio web de DMTF en **www.dmtf.org**.

El ejemplo siguiente muestra cómo incluir el contenido del registro de sucesos del sistema en el mensaje de salida de XML:

```
show -l all -output format=clpxml /system1/sp1/logs1
```

Ejemplos de SM-CLP del iDRAC

Los apartados siguientes contienen ejemplos para usar el SM-CLP para ejecutar las operaciones siguientes:

- Administración de la alimentación del servidor
- Administración del registro de sucesos del sistema
- Navegación del mapa de destino
- Mostrar las propiedades del sistema
- Establecimiento de la dirección IP, la máscara de subred y la dirección de puerta de enlace del iDRAC

Para información sobre el uso de la interfaz SM-CLP de iDRAC, consulte Base de datos de propiedades iDRAC SMCLP.

Administración de la alimentación del servidor

La tabla 11-4 contiene ejemplos de cómo usar el SM-CLP para realizar operaciones de administración de la alimentación del servidor en un servidor administrado.

Tabla 11-4. Operaciones de administración de la alimentación del servidor

Operación	Sintaxis
Iniciar sesión en el iDRAC por medio de la interfaz SSH	`>ssh 192.168.0.120` `>login: root` `>password:`
Apagar el servidor	`->stop /system1` `system1 se ha detenido correctamente`
Encender el servidor a partir de un estado apagado	`->start /system1` `system1 se ha iniciado correctamente`
Reiniciar el servidor	`->reset /system1`

	system1 se ha restablecido correctamente

Administración del registro de sucesos del sistema

La tabla 11-5 contiene ejemplos de cómo usar el SM-CLP para ejecutar operaciones relacionadas con el registro de sucesos del sistema en el sistema administrado.

Tabla 11-5. Operaciones de administración del registro de sucesos del sistema

Operación	Sintaxis
Ver el registro de sucesos del sistema	->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: cd delete exit help show version
Ver la anotación del registro de sucesos del sistema	->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version
Borrar el registro de sucesos del sistema	->delete /system1/sp1/logs1 All records deleted successfully

Navegación del MAP de destino

La tabla 11-6 muestra ejemplos de cómo usar el verbo **cd** para navegar el MAP. En todos los ejemplos, se supone que el destino inicial predeterminado es /.

Tabla 11-6. Operaciones de navegación del mapa de destino

Operación	Sintaxis
Navegar hacia el sistema destino y reiniciar	->cd system1 ->reset **NOTA:** El destino predeterminado actual es /.
Navegar hacia el registro de sucesos del sistema de destino y mostrar las anotaciones del registro	->cd system1 ->cd sp1 ->cd logs1 ->show
	->cd system1/sp1/logs1 ->show
Mostrar el destino actual	->cd .
Subir un nivel	->cd ..

Salir del shell	`->exit`

Establecimiento de la dirección IP, la máscara de subred y la dirección de puerta de enlace del iDRAC

El uso de SM-CLP para actualizar las propiedades de la red de iDRAC es un proceso de dos partes:

1. Establezca los nuevos valores de las propiedades de NIC en la ubicación **/system1/sp1/enetport1/lanendpt1/ipendpt1:**
   - **oemdell_nicenable**: definir como 1 para activar el sistema de red del iDRAC y 0 para desactivarlo
   - **ipaddress**: la dirección IP
   - **subnetmask**: la máscara de subred
   - **oemdell_usedhcp**: establezca como 1 para activar el uso de DHCP para definir las propiedades **ipaddress** y **subnetmask**, 0 para establecer valores estáticos
2. Aplique los nuevos valores asignando un valor de 1 a la propiedad **committed**.

Siempre que la propiedad **commit** tenga el valor de 1, los valores actuales de las propiedades estarán activados. Cuando usted cambia alguna de las propiedades, la propiedad **commit** se restablece y recibe el valor de 0 para indicar que los valores no se han aplicado.

NOTA: La propiedad **commit** sólo afecta las propiedades en la ubicación de MAP **/system1/sp1/enetport1/lanendpt1/ipendpt1**. Todos los demás comandos de SM-CLP surten efecto inmediatamente.

NOTA: Si utiliza RACADM local para definir las propiedades de red del iDRAC, los cambios surtirán efecto inmediatamente, pues RACADM local no depende de una conexión de red.

Cuando usted aplica los cambios, la nueva configuración de la red surte efecto, lo que hace que la sesión Telnet o SSH termine. Si incluye el paso de la opción commit, puede retrasar la terminación de la sesión hasta que haya terminado todos los comandos de SM-CLP.

La tabla 11-7 muestra ejemplos de cómo establecer las propiedades del iDRAC por medio de SM-CLP.

Tabla 11-7. Configuración de las propiedades de red del iDRAC con SM-CLP

Operación	Sintaxis
Desplazarse a la ubicación de las propiedades de la NIC del iDRAC	`->cd /system1/sp1/enetport1/lanendpt1/ipendpt1`
Establecer la nueva dirección IP	`->set ipaddress=10.10.10.10`
Establecer la máscara de subred	`->set subnetmask=255.255.255.255`
Activar el indicador de DHCP	`->set oemdell_usedhcp=1`
Activar la tarjeta de interfaz de red	`->set oemdell_nicenable=1`
Aplicar los cambios	`->set committed=1`

Actualización del firmware del iDRAC por medio de SM-CLP

Para actualizar el firmware del iDRAC por medio de SM-CLP, se debe conocer el URI de TFTP para el paquete de actualización de Dell.

Siga estos pasos para actualizar el firmware por medio de SM-CLP:

1. Inicie sesión en el iDRAC por medio de Telnet o SSH.
2. Revise la versión del firmware actual con el comando siguiente:

   ```
   version
   ```

3. Introduzca el comando siguiente:

   ```
   load -source tftp://<servidor_tftp>/<ruta_de_acceso_de_actualización> /system1/sp1
   ```

   donde *<servidor_tftp>* es el nombre DNS o la dirección IP del servidor TFTP y *<ruta_de_acceso_de_actualización>* es la ruta de acceso al paquete de actualización en el servidor TFTP.

   La sesión de Telnet o SSH se finalizará. Es posible que deba esperar varios minutos a que la actualización del firmware concluya.

4. Para verificar que se ha escrito el nuevo firmware, inicie una nueva sesión de Telnet o SSH y vuelva a introducir el comando de versión.

Uso de la comunicación en serie en la LAN (SOL) con Telnet o SSH

Utilice una consola Telnet o SSH en su estación de administración para conectarse al iDRAC y después redirija el puerto en serie del servidor administrado hacia la consola. Esta función es una alternativa a la comunicación en serie en la LAN de IPMI, la cual requiere que una utilidad como **solproxy** traduzca la comunicación en serie en paquetes de red. La implementación de la SOL de iDRAC elimina la necesidad de tener una utilidad adicional pues la traducción de la comunicación en serie a comunicación de red se realiza dentro del iDRAC.

La consola de Telnet o SSH que usted utiliza deberá ser capaz de interpretar y responder a los datos provenientes del puerto serie del servidor administrado. El puerto serie por lo general se conecta a un shell que emula una terminal ANSI o VT100.

A través de Telnet, usted se conecta al puerto de comunicación en serie en la LAN de IPMI: el puerto 2100. La consola en serie se redirige automáticamente a la consola de Telnet.

Con SSH o Telnet, usted se conecta al iDRAC de la misma manera que se conecta a SM-CLP. La redirección de la comunicación en serie en la LAN se puede iniciar desde el destino **/system1/sol1**.

Consulte Instalación de clientes Telnet o SSH para obtener más información sobre cómo usar clientes Telnet y SSH con el iDRAC.

Uso de la comunicación en serie en la LAN por medio de Telnet con HyperTerminal de Microsoft Windows

1. Seleccione **Inicio**→ **Todos los programas**→ **Accesorios**→ **Comunicaciones**→ **HyperTerminal**.
2. Introduzca un nombre para la conexión, elija un icono y haga clic en **Aceptar**.
3. Elija **TCP/IP (Winsock)** en la lista del campo **Conectar usando**.
4. Introduzca el nombre DNS o la dirección IP del iDRAC en el campo **Dirección del host**.
5. Introduzca el número del puerto Telnet en el campo **Número de puerto**.
6. Haga clic en **Aceptar**.

Para terminar la sesión de comunicación en serie en la LAN, haga clic en el símbolo para desconectar de HyperTerminal.

Uso de la comunicación en serie en la LAN mediante Telnet con Linux

Para iniciar la comunicación en serie en la LAN por medio de Telnet en una estación de administración con Linux, siga estos pasos:

1. Inicie una ventana de shell.
2. Conéctese al iDRAC con el comando siguiente:

   ```
   telnet <dirección_IP_del_iDRAC>
   ```

   NOTA: Si cambió el número predeterminado de puerto del servicio de Telnet, el puerto 23, agregue el número de puerto al final del comando **telnet**.

3. Introduzca el siguiente comando para iniciar la comunicación en serie en la LAN:

   ```
   start /system1/sol1
   ```

   Con esto se conectará al puerto serie del servidor administrado.

Cuando esté listo para cerrar la SOL, escriba <Ctrl>+] (mantenga presionada la tecla Ctrl, presione y suelte la tecla de corchete de cierre y luego suelte Ctrl). Aparecerá una petición de Telnet. Escriba quit para salir de Telnet.

Uso de SOL por medio de SSH

El destino **/system1/sol1** permite redirigir el puerto serie del servidor administrado hacia la consola SSH.

1. Conéctese al iDRAC por medio de OpenSSH o PuTTY.
2. Introduzca el siguiente comando para iniciar la SOL:

   ```
   start /system1/sol1
   ```

Con esto se conectará al puerto en serie del servidor administrado. Los comandos de SM-CLP ya no estarán disponibles para usted.

Cuando esté listo para salir de la redirección de SOL, presione <Entrar>, <Esc> y después <T> (presione las teclas en secuencia, una tras otra). La sesión de SSH se cerrará.

Una vez que haya iniciado la SOL, no podrá regresar a SM-CLP. Deberá salir de la sesión SSH e iniciar una nueva sesión para poder usar SM-CLP.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación del sistema operativo por medio de iVM-CLI

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

La utilidad de interfaz de línea de comandos de medios virtuales (iVM-CLI) es una interfaz de línea de comandos que ofrece las funciones de medios virtuales de la estación de administración al iDRAC en el sistema remoto. Por medio de la iVM-CLI y los métodos con secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad iVM-CLI en su red corporativa.

Antes de comenzar

Antes de usar la utilidad iVM-CLI, asegúrese de que los sistemas remotos de destino y la red de la empresa cumplan con los requisitos que se listan en las secciones siguientes.

Requisitos de los sistemas remotos

- El iDRAC se configura en cada sistema remoto.

Requisitos de red

Una área compartida de red debe tener los componentes siguientes:

- Los archivos de sistema operativo
- Los controladores necesarios
- El(los) archivo(s) de imagen de inicio del sistema operativo

  El archivo de imagen debe ser un CD de sistema operativo o una imagen ISO de CD/DVD, con un formato de inicio estándar en la industria.

Creación de un archivo de imagen de inicio

Antes de instalar el archivo de imagen en los sistemas remotos, compruebe que el sistema compatible pueda iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz de usuario web de iDRAC y luego reinicie el sistema.

Las secciones siguientes contienen información específica para la creación de archivos de imagen para los sistemas Linux y Windows.

Creación de un archivo de imagen para los sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen iniciable para el sistema Linux.

Para ejecutar la utilidad, abra una petición de comandos y escriba lo siguiente:

```
dd if=<dispositivo_de_entrada> of=<archivo_de_salida>
```

Por ejemplo:

```
dd if=/dev/sdc0 of=mycd.img
```

Creación de un archivo de imagen para los sistemas Windows

Al elegir una utilidad duplicadora de datos para los archivos de imagen de Windows, seleccione una utilidad que copie el archivo de imagen y los sectores de inicio de CD/DVD.

Preparación para la instalación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que la Management Station pueda acceder.
2. Copie los archivos de sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen iniciable preconfigurado para instalación, cree el archivo. Incluya los programas o secuencias de comandos que se vayan a utilizar para los procedimientos de instalación del sistema operativo.

   Por ejemplo, para implementar un sistema operativo Microsoft® Windows®, el archivo de imagen puede incluir programas que sean parecidos a los métodos de implementación que utiliza Microsoft Systems Management Server (SMS).

   Al momento de crear el archivo de imagen, haga lo siguiente:

   - Siga los procedimientos estándares de instalación basada en red
   - Marque la imagen de instalación como "de sólo lectura" para garantizar que cada sistema de destino se inicie y se ejecute en el mismo procedimiento de instalación

- Realice uno de los procedimientos siguientes:
  - Integre **ipmitool** y la interfaz de línea de comandos de medios virtuales (iVM-CLI) en la aplicación existente de instalación del sistema operativo. Use la secuencia de comandos de ejemplo **ivmdeploy** como guía para usar la utilidad.
  - Utilice la secuencia de comandos **ivmdeploy** existente para instalar el sistema operativo.

Instalación del sistema operativo

Use la utilidad iVM-CLI y la secuencia de comandos **ivmdeploy** que se incluye con la utilidad para instalar el sistema operativo en los sistemas remotos.

Antes de comenzar, revise la secuencia de comandos **ivmdeploy** de ejemplo que se incluye con la utilidad iVM-CLI. La secuencia de comandos muestra los pasos detallados que se necesitan para instalar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para instalar el sistema operativo en los sistemas remotos de destino.

1. Haga una lista de las direcciones IP de iDRAC de los sistemas remotos que serán instalados en el archivo de texto **ip.txt**, una dirección IP por línea.
2. Inserte un CD o DVD iniciable de sistema operativo en la unidad correspondiente del cliente.
3. Ejecute **ivmdeploy** en la línea de comandos.

Para ejecutar la secuencia de comandos ivmdeploy, introduzca el siguiente comando en el símbolo del sistema:

```
ivmdeploy -r ip.txt -u <usuario_del_idrac> -p <contraseña_del_idrac> -c {<imagen_iso9660> | <ruta_de_acceso>}
```

donde:

- <*usuario_del_idrac*> es el nombre de usuario del iDRAC, por ejemplo, **root**
- <*contraseña_del_idrac*> es la contraseña del usuario del iDRAC, por ejemplo, **calvin**
- <*imagen_iso9660*> es la ruta de acceso de la imagen ISO9660 del CD o DVD de instalación del sistema operativo
- <*ruta_de_acceso*> es la ruta de acceso del dispositivo que contiene el CD o DVD de instalación del sistema operativo

La secuencia de comandos **ivmdeploy** pasa las opciones de línea de comandos a la utilidad **iVMCLI**. Consulte Opciones de la línea de comandos para obtener detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta a la opción **iVMCLI -r**. Si el argumento de la opción **-r** es el nombre de un archivo existente, la secuencia de comandos leerá las direcciones IP de iDRAC del archivo especificado y ejecutará la utilidad **iVMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, deberá ser la dirección de un solo iDRAC. En este caso, la opción **-r** funciona como se describe en la utilidad **iVMCLI**.

La secuencia de comandos ivmdeploy admite únicamente instalaciones a partir de un CD/DVD o de una imagen ISO9660 de CD/DVD. Si necesita instalar a partir de un disco flexible o de una imagen de disco flexible, puede modificar la secuencia de comandos para usar la opción **iVMCLI -f**.

Uso de la utilidad de interfaz de línea de comandos de los medios virtuales

La utilidad de interfaz de línea de comandos de medios virtuales (iVM-CLI) es una interfaz de línea de comandos que se puede usar con secuencias de comandos y que suministra las funciones de medios virtuales de la estación de administración al iDRAC.

La utilidad iVM-CLI ofrece las siguientes características:

NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.

- Dispositivos de medios extraíbles o archivos de imagen que son congruentes con los complementos de medios virtuales
- Terminación automática cuando la opción para iniciar una vez del firmware de iDRAC está activada
- Comunicaciones seguras con el iDRAC por medio de la Capa de conexión segura (SSL)

Antes de que ejecutar la utilidad, compruebe que cuenta con privilegios de usuario de medios virtuales en el iDRAC.

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 iVM-CLI.

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 iVM-CLI.

En los sistemas Linux, se puede acceder a la utilidad iVM-CLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando brinda un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos del usuario. Para agregar o editar usuarios en el grupo iVM-CLI, 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 iVM-CLI (o a la secuencia de comandos de iVM-CLI) a fin de obtener acceso al iDRAC en el sistema remoto y ejecutar la utilidad.

Instalación de la utilidad iVM-CLI

La utilidad iVM-CLI se encuentra en el CD *Dell OpenManage™ Systems Management Consoles*, que está incluido en el paquete de software de Dell OpenManage System Management. Para instalar la utilidad, inserte el CD *System Management Consoles* en la unidad de CD del sistema y siga las instrucciones que aparecen en la pantalla.

El CD *Systems Management Consoles* contiene los productos de software de administración de sistemas más recientes, incluyendo diagnósticos, administración de almacenamiento, servicio de acceso remoto y la utilidad RACADM. Este CD también contiene archivos readme (léame) con la información más reciente sobre los productos de software de administración de sistemas.

El CD *Systems Management Consoles* incluye el archivo **ivmdeploy**; una secuencia de comandos de muestra que ilustra cómo usar las utilidades iVM-CLI y RACADM para instalar el software en varios sistemas remotos.

NOTA: La secuencia de comandos **ivmdeploy** depende de otros archivos que están presentes en el directorio de la misma cuando se instala. Si desea usar la secuencia de comandos desde otro directorio, deberá copiar todos los archivos con ella.

Opciones de la línea de comandos

La interfaz iVM-CLI es idéntica en los sistemas Windows y Linux. La utilidad usa opciones que son congruentes con las opciones de la utilidad RACADM. Por ejemplo, una opción para especificar la dirección IP de iDRAC requiere la misma sintaxis tanto en la utilidad RACADM como en la utilidad iVM-CLI.

El formato del comando de iVM-CLI es como se indica a continuación:

```
iVMCLI [parámetro] [opciones_de_shell_de_sistema_operativo]
```

En la sintaxis de la línea de comandos se distingue entre mayúsculas y minúsculas. Consulte "Parámetros de iVM-CLI" para obtener más información.

Si el sistema remoto acepta los comandos y el iDRAC autoriza la conexión, el comando seguirá ejecutándose hasta que se presente cualquiera de los siguientes casos:

- La conexión de iVM-CLI 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 iVM-CLI

Dirección IP del iDRAC

```
-r <Dirección_IP_de_iDRAC>[:<puerto_SSL_de_iDRAC>]
```

Este parámetro proporciona la dirección IP del iDRAC y el puerto SSL, con los que la utilidad debe establecer una conexión de medios virtuales con el iDRAC de destino. Si introduce un nombre de DDNS o una dirección IP no válida, aparecerá un mensaje de error y el comando terminará.

donde <*dirección_IP_de_iDRAC*> es una dirección IP válida y única, o bien, el nombre de Sistema dinámico de nombres de dominio (DDNS) de iDRAC (si se admite). Si se omite <*Puerto_SSL_de_iDRAC*>, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado de iDRAC.

Nombre de usuario del iDRAC

```
-u <nombre_de_usuario_del_iDRAC>
```

Este parámetro proporciona el nombre de usuario de iDRAC que ejecutará los medios virtuales.

El <*nombre_de_usuario_de_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales de iDRAC

Si la autentificación de iDRAC falla, aparecerá un mensaje de error y se finalizará el comando.

Contraseña de usuario del iDRAC

`-p` *<contraseña_de_usuario_del_iDRAC>*

Este parámetro proporciona la contraseña para el usuario de iDRAC especificado.

Si la autenticación de iDRAC falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco / disco flexible

`-f {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido, incluyendo el número de partición del sistema de archivos montable, de ser aplicable (para sistemas Linux); y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

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)

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, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD / DVD

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o archivo que proporcionará el medio virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

`-c c:\temp\mydvd.img` (sistemas Windows)

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Windows)

`-c /dev/cdrom` (sistemas Linux)

Omita este parámetro de la línea de comandos si no va a virtualizar discos CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de conmutador. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

-v

Este parámetro se usa para mostrar la versión de la utilidad iVM-CLI. Si no se proporcionan otras opciones además de conmutadores, el comando terminará sin mensajes de error.

Mostrar la ayuda

-h

Este parámetro muestra un resumen de los parámetros de la utilidad iVM-CLI. Si no se proporcionan otras opciones además de conmutadores, el comando terminará sin errores.

Consulta del manual

-m

Este parámetro muestra una "página de manual" detallada de la utilidad iVM-CLI, incluso las descripciones de todas las opciones posibles.

Datos cifrados

-e

Cuando se incluya este parámetro en la línea de comandos, iVM-CLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el iDRAC en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifrará.

Opciones de shell de sistema operativo de iVM-CLI

Las siguientes funciones del sistema operativo se pueden usar en la línea de comandos de iVM-CLI:

- stderr/stdout redirection: desvía los mensajes de salida impresos de la utilidad hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad iVM-CLI.

  NOTA: La utilidad VM-CLI no lee la entrada estándar (**stdin**). En consecuencia, la redirección de **stdin** no es necesaria.

- Ejecución en segundo plano: de manera predeterminada, la utilidad iVM-CLI se ejecuta en primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en el segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter et (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

La última técnica es útil en programas de secuencias de comandos, ya que permite que la secuencia de comandos proceda después de que se inicia un nuevo proceso para el comando iVM-CLI (de lo contrario, la secuencia de comandos se bloqueará hasta que el programa iVM-CLI finalice). Cuando se inician varias instancias de iVM-CLI de esta manera, y una o varias de las instancias de comando se finalizan manualmente, utilice las instalaciones específicas del sistema operativo para listar y finalizar procesos.

Códigos de retorno de iVM-CLI

0 = Sin errores

1 = No se puede conectar

2 = Error de línea de comandos de iVM-CLI

3 = Se cerró la conexión del firmware del RAC

Cuando se presentan errores, también se envían mensajes de texto en inglés a la salida estándar de errores.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la utilidad de configuración del iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Información general

La utilidad de configuración del iDRAC es un entorno de configuración previo al inicio que permite ver y establecer parámetros del iDRAC y del servidor administrado. Expresamente, usted puede:

- Ver los números de revisión del firmware del iDRAC y del firmware de la tarjeta primaria de plano posterior
- Configurar, activar o desactivar la red de área local del iDRAC
- Activar o desactivar la IPMI en la LAN
- Activar un destino de captura de sucesos de plataforma (PET) de la LAN
- Conectar o desconectar los dispositivos de medios virtuales
- Cambiar el nombre de usuario administrativo y la contraseña
- Restablecer la configuración predeterminada de fábrica del iDRAC
- Ver o borrar los mensajes del registro de sucesos del sistema (SEL)

Las tareas que puede realizar con la utilidad de configuración del iDRAC también pueden realizarse mediante otras utilidades que se incluyen con el iDRAC o el software OpenManage, incluyendo la interfaz web, la interfaz de línea de comandos de SM-CLP, la interfaz de línea de comandos de RACADM local y, en el caso de la configuración de red básica, en la pantalla LCD del CMC durante la configuración inicial del CMC.

Inicio de la utilidad de configuración del iDRAC

Se debe usar una consola conectada al iKVM para tener acceso a la utilidad de configuración del iDRAC al inicio o después de restablecer la configuración predeterminada del iDRAC.

1. En el teclado conectado a la consola iKVM, presione <Impr Pant> para mostrar el menú de OSCAR (On Screen Configuration and Reporting) del iKVM. Use las teclas de <Flecha ascendente> y <Flecha descendente> para resaltar la ranura que contiene el servidor y después presione <Entrar>.
2. Encienda o reinicie el servidor con el botón de encendido que se encuentra en el frente del servidor.
3. Cuando aparezca el mensaje **Presione <Ctrl-E> para la configuración de acceso remoto dentro de 5 segundos.....**, presione inmediatamente <Ctrl><E>.

NOTA: Si el sistema operativo comienza a cargarse antes de que usted presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el servidor e inténtelo otra vez.

Aparecerá la utilidad de configuración del iDRAC. Las dos primeras líneas ofrecen información sobre el firmware del iDRAC y las revisiones del firmware de la tarjeta primaria de plano posterior. Los niveles de revisión pueden ser útiles para determinar si una actualización de firmware es necesaria.

El firmware del iDRAC es la parte del firmware que se encarga de las interfaces externas, por ejemplo, la interfaz web, SM-CLP y las interfaces web. El firmware de la tarjeta primaria de plano posterior es la parte del firmware que se conecta y supervisa el entorno de hardware del servidor.

Uso de la utilidad de configuración del iDRAC

Bajo los mensajes de revisión de firmware, el resto de la utilidad de configuración del iDRAC es un menú de opciones a las que puede tener acceso por medio de las teclas de <Flecha ascendente> y <Flecha descendente>.

- Si una opción del menú conduce a un submenú o a un campo de texto editable, presione <Entrar> para acceder a la opción y <Esc> para salir de la misma después de terminar de configurarla.
- Si un elemento tiene valores que se pueden seleccionar, como Sí/No o Activado/Desactivado, presione <Flecha hacia la izquierda>, <Flecha hacia la derecha> o <Barra espaciadora> para elegir un valor.
- Si un elemento no se puede editar, aparecerá en azul. Algunos elementos se pueden editar en función de otras selecciones que usted haga.
- La línea en la parte inferior de la pantalla muestra instrucciones relacionadas con el elemento actual. Puede presionar <F1> para mostrar la ayuda del elemento actual.
- Cuando haya terminado de usar la utilidad de configuración del iDRAC, presione <Esc> para 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 iDRAC.

LAN

Use la <Flecha hacia la izquierda>, la <Flecha hacia la derecha> y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**.

La LAN del iDRAC está desactivada en la configuración predeterminada. Es necesario activar la LAN para permitir el uso de los servicios del iDRAC, como la interfaz web, el acceso Telnet/SSH a la interfaz de línea de comandos de SM-CLP, la redirección de consola y los medios virtuales.

Si elige desactivar la LAN, aparecerá la siguiente advertencia:

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (La interfaz del iDRAC fuera de banda se desactivará si el canal de LAN está desactivado.)`

`Press any key to clear the message and continue. (Presione cualquier tecla para quitar el mensaje y continuar.)`

El mensaje le informa que, además de los servicios a los que tiene acceso a través de la conexión directa del iDRAC, HTTP, HTTPS, Telnet o los puertos SSH, el tráfico de red de administración fuera de banda, por ejemplo, los mensajes de IPMI que se envían al iDRAC desde una estación de administración, no se recibe cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN de iDRAC.

IPMI en la LAN (Activada/Desactivada)

Presione la <Flecha hacia la izquierda>, <Flecha hacia la derecha> y la barra espaciadora para elegir entre **Activada** y **Desactivada**. Cuando se seleccione **Desactivada**, el iDRAC no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivada**, aparecerá la siguiente advertencia:

`iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF. (La interfaz del iDRAC fuera de banda se desactivará si el canal de LAN está desactivado.)`

Presione cualquier tecla para quitar el mensaje y continuar. Consulte LAN para ver una explicación del mensaje.

Parámetros de LAN

Presione <Entrar> para mostrar el submenú de parámetros de la LAN. Cuando haya terminado de configurar los parámetros de la LAN, presione <Esc> para volver al menú anterior.

Tabla 13-1. Parámetros de LAN

Elemento	Descripción
Clave de cifrado de RMCP+	Presione <Entrar> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado de 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.
Fuente de dirección IP	Seleccione entre **DHCP** y **Estática**. Cuando se selecciona DHCP, los campos **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se obtienen de un servidor DHCP. Si no se encuentra ningún servidor DHCP en la red, los campos tomarán valores de ceros. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar**.**
Dirección IP de Ethernet	Si la opción **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC. El valor predeterminado es **192.168.0.120** más el número de la ranura que contiene el servidor.
Dirección MAC	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC.
Máscara de subred	Si la **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección de máscara de subred que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la máscara de subred para el iDRAC. El valor predeterminado es **255.255.255.0**.
Puerta de enlace predeterminada	Si la **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada. El valor predeterminado es **192.168.0.1**.
Alerta de LAN activada	Seleccione **Activada** para activar la alerta de captura de sucesos de plataforma (PET) de LAN.
Anotación de política de alerta 1	Seleccione Activar o Desactivar para activar el primer destino de alerta.
Destino de alerta 1	Introduzca la dirección IP a la que se enviarán las alertas de captura de sucesos de plataforma de la LAN.
Cadena de nombre del	Presione <Entrar> para editarla. Introduzca el nombre del host para las alertas de captura de sucesos de plataforma.

host	
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidor DNS. Seleccione **Desactivado** para especificar las direcciones de servidor 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.
Registrar el nombre del iDRAC	Seleccione **Activado** para registrar el nombre del iDRAC en el servicio DNS. Seleccione **Desactivado** si no desea que los usuarios puedan encontrar el nombre del iDRAC en el DNS.
Nombre del iDRAC	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Entrar> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Presione <Entrar> cuando haya terminado de modificar el nombre del iDRAC. Presione <Esc> para volver al menú anterior. El nombre del iDRAC debe ser un nombre de host válido de DNS.
Nombre de dominio de DHCP	Seleccione **Activado** si desea obtener el nombre de dominio de un servicio DHCP de la red. Seleccione **Desactivado** si desea especificar el nombre de dominio.
Nombre de dominio	Si **Nombre de dominio de DHCP** esta **Desactivado**, presione <Entrar> para modificar el campo de texto **Nombre de dominio actual**. Presione <Entrar> cuando haya terminado de modificarlo. Presione <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.

Medios virtuales

Use la <Flecha hacia la izquierda> y la <Flecha hacia la derecha> para seleccionar **Conectado** o **Desconectado**. Cuando se selecciona **Conectado**, los dispositivos de medios virtuales se conectan al bus USB y están listos para su uso durante las sesiones de **Redirección de consola**.

Si selecciona **Desconectado**, los usuarios no podrán acceder a los dispositivos de medios virtuales durante las sesiones de **Redirección de consola**.

NOTA: Para usar una unidad flash USB con la función de **Medios virtuales**, la opción **Tipo de emulación de unidad flash USB** debe estar establecida como **Disco duro** en la utilidad de configuración del BIOS. Se puede acceder a la utilidad de configuración del BIOS al presionar <F2> durante el arranque del servidor. Si el **Tipo de emulación de la unidad flash USB** se establece como **Automático**, la unidad flash aparecerá como unidad de disco flexible en el sistema.

Configuración de usuario de la LAN

El usuario de la LAN es la cuenta de administrador del iDRAC, que tiene el nombre predeterminado **root**. Presione <Entrar> para mostrar el submenú de configuración de usuario de la LAN. Cuando haya terminado de configurar el usuario de la LAN, presione <Esc> para volver al menú anterior.

Tabla 13-2. Página de configuración de usuarios de la LAN

Elemento	Descripción
Acceso de cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione **Desactivado** para desactivar la cuenta de administrador.
Privilegio de cuenta	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Entrar> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Escriba la nueva contraseña para la cuenta de administrador. Los caracteres no aparecerán en la pantalla cuando usted los escriba.
Confirmar la contraseña	Escriba nuevamente la nueva contraseña para la cuenta de administrador. Si los caracteres que introduzca no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparecerá un mensaje y usted deberá introducir nuevamente la contraseña.

Restablecer valores predeterminados

Use la opción de menú **Restablecer valores predeterminados** para restablecer todos los valores predeterminados de fábrica de las opciones de configuración del iDRAC. Esto puede ser necesario, por ejemplo, cuando usted ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC a partir de los valores predeterminados.

NOTA: En la configuración predeterminada, el sistema de red del iDRAC está desactivado. Usted no podrá reconfigurar el iDRAC por medio de la red hasta que haya activado la red del iDRAC en la utilidad de configuración del iDRAC.

Presione <Entrar> para seleccionar el elemento. Aparecerá el siguiente mensaje de advertencia:

`Resetting to factory defaults will restore remote Non-Volatile user settings. Continue? (Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Continuar?)`

`< NO (Cancelar) >`

`< SÍ (Continuar) >`

Seleccione **SÍ** y presione <Entrar> para restablecer los valores predeterminados del iDRAC.

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 <Entrar> para mostrar el

Menú del registro de sucesos del sistema. El sistema cuenta las anotaciones del registro y después muestra el número total de anotaciones y el mensaje más reciente. El registro de sucesos del sistema retiene un máximo de 512 mensajes.

Para ver los mensajes del registro de sucesos del sistema, seleccione **Ver registro de sucesos del sistema** y presione <Entrar>. Use la <Flecha hacia la izquierda> para retroceder al mensaje anterior (más antiguo) y <Flecha hacia la 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 de registro de sucesos del sistema.

NOTA: Sólo puede borrar el registro de sucesos del sistema en la utilidad de configuración del iDRAC o en la interfaz web del iDRAC.

Para borrar el registro de sucesos del sistema, seleccione **Borrar el registro de sucesos del sistema** y presione <Entrar>.

Cuando haya terminado con el menú de registro de sucesos del sistema, presione <Esc> para volver al menú anterior.

Cómo salir de la utilidad de configuración del iDRAC

Cuando haya terminado de hacer cambios en la configuración del iDRAC, presione la tecla <Esc> para mostrar el menú de salida.

Seleccione **Guardar cambios y salir** y presione <Entrar> para retener los cambios.

Seleccione **Descartar cambios y salir** y presione <Entrar> para ignorar los cambios que ha realizado.

Seleccione **Regresar a la configuración** y presione <Entrar> para volver a la utilidad de configuración del iDRAC.

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del servidor administrado

Guía del usuario de Integrated Dell™ Remote Access Controller
versión 1.2

Esta sección explica cómo realizar tareas relacionadas con el diagnóstico y la solución de problemas de un servidor administrado remoto por medio de los servicios de iDRAC. Contiene los apartados siguientes:

- Indicadores de problemas: ayuda a encontrar mensajes y otros indicadores del sistema que pueden conducir a un diagnóstico del problema
- Herramientas para solución de problemas: describe las herramientas de iDRAC que se pueden usar para solucionar problemas del sistema
- Solución de problemas y preguntas frecuentes: respuestas a situaciones típicas que usted puede encontrar

---

La seguridad es lo primero; para usted y su sistema

Para realizar ciertos procedimientos de esta sección, se debe trabajar con el chasis, el servidor PowerEdge u otros módulos de hardware. No intente reparar el hardware del sistema salvo según se explica en esta guía y en otra parte en la documentación del sistema.

⚠ **PRECAUCIÓN: Muchas de las reparaciones deben realizarlas únicamente los técnicos de servicio autorizados. Usted sólo deberá aplicar las soluciones de problemas y reparaciones simples que se autoricen en la documentación del producto o según lo indique el equipo de asistencia técnica por teléfono o en línea. La garantía no cubre los daños ocasionados por reparaciones que Dell no haya autorizado. Lea y siga las instrucciones de seguridad entregadas con el producto.**

Indicadores de problemas

Esta sección describe indicadores que sugieren que puede haber un problema en el sistema.

Indicadores LED

La señal inicial de la existencia de un problema del sistema pueden ser los indicadores LED del chasis o de los componentes instalados en el chasis. Los siguientes componentes y módulos tienen indicadores LED de estado:

- Pantalla LCD del chasis
- Servidores
- Ventiladores
- CMC
- Módulos de E/S
- Fuentes de alimentación

El indicador LED de la pantalla LCD del chasis resume el estado de todos los componentes del sistema. Un LED de color azul indica que no se han detectado condiciones de falla en el sistema. Si el LED parpadea en color ámbar, indica que se han detectado una o más condiciones de falla.

Si la pantalla LCD del chasis tiene un LED que parpadea en color ámbar, se puede usar el menú de la pantalla LCD para localizar el componente que tiene la falla. Consulte la *Guía del usuario del firmware del CMC Dell* para ayuda sobre la utilización de la pantalla LCD.

La tabla 14-1 describe el significado del comportamiento del indicador LED del servidor PowerEdge:

Tabla 14-1. Indicadores LED del servidor

Indicador LED	Significado
verde continuo	El servidor está encendido. La ausencia del indicador LED en color verde significa que el servidor no está encendido.
azul continuo	El iDRAC presenta una condición satisfactoria.
parpadeo en color ámbar	El iDRAC ha detectado una condición de falla o es posible que esté en proceso de actualizar el firmware.
parpadeo en color azul	Un usuario ha activado la identificación de localizador de este servidor.

Indicadores de problemas del hardware

Los indicadores de que un módulo tiene un problema de hardware incluyen los siguientes:

- Falla de encendido
- Ventiladores ruidosos
- Pérdida de conectividad de red
- Alertas de los sensores de supervisión de la batería, temperatura, voltaje o alimentación
- Fallas de disco duro
- Falla de medios USB
- Daños físicos provocados por caídas, agua u otros agentes externos

Cuando se presentan estos tipos de problemas, puede intentar corregir el problema con estas estrategias:

- Reasiente el módulo y reinícielo
- Inserte el módulo en otro compartimiento del chasis
- Sustituya los discos duros o memorias USB
- Vuelva a conectar o reemplace los cables de alimentación y de red

Si estos pasos no corrigen el problema, consulte el *Manual del propietario del hardware* para obtener información específica de solución de problemas del dispositivo de hardware.

Otros indicadores de problemas

Tabla 14-2. Indicadores de problemas

Buscar:	**Acción:**
Mensajes de alerta procedentes del software de administración de sistemas	Consulte la documentación del software de administración de sistemas.
Mensajes en el registro de sucesos del sistema	Consulte el apartado Consulta del registro de sucesos del sistema (SEL).
Mensajes en los códigos POST de inicio	Consulte el apartado Consulta de los códigos POST.
Mensajes en la pantalla de último bloqueo	Consulte el apartado Visualización de la pantalla de último bloqueo del sistema.
Mensajes de alerta en la pantalla de estado del servidor de la LCD	Consulte el apartado Consulta de la pantalla de estado del sistema en busca de mensajes de error.
Mensajes en el registro del iDRAC	Consulte el apartado Visualización del registro del iDRAC.

Herramientas para solución de problemas

Esta sección describe los servicios del iDRAC que se pueden usar para diagnosticar problemas del sistema, sobre todo cuando usted trata de solucionar problemas de manera remota.

- Consulta de la condición del sistema
- Consulta del registro de sucesos del sistema en busca de mensajes de error
- Consulta de los códigos POST
- Visualización de la pantalla de último bloqueo
- Consulta de la pantalla de estado del servidor en la pantalla LCD en busca de mensajes de error
- Visualización del registro del iDRAC
- Acceso a la información del sistema
- Identificación del servidor administrado en el chasis
- Uso de la consola de diagnósticos
- Administración de alimentación en un sistema remoto

Consulta de la condición del sistema

Al iniciar sesión en la interfaz web del iDRAC, la primera página que aparece describe la condición de los componentes del sistema. La tabla 14-3 describe el significado de los indicadores de condición del sistema.

Tabla 14-3. Indicadores de condición del sistema

Indicador	Descripción
	Una marca de verificación verde indica una condición de estado sana (normal).
	Un triángulo amarillo que contiene un signo de admiración indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.

Haga clic en cualquier componente en la página **Condición** para ver la información sobre el componente. Se muestran las lecturas de sensores de baterías, temperaturas, voltajes y supervisión de alimentación, lo que ayuda a diagnosticar algunos tipos de problemas. Las páginas de información del iDRAC y el CMC muestran información útil sobre el estado actual y la configuración.

Consulta del registro de sucesos del sistema (SEL)

La página **Registro SEL** muestra los mensajes de los sucesos que ocurren en el servidor administrado.

Para ver el **Registro de sucesos del sistema**, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Registros**.

2. Haga clic en **Registro de sucesos del sistema** para mostrar la página **Registro de sucesos del sistema**.

   La página **Registro de sucesos del sistema** muestra un indicador de condición del sistema (consulte la tabla 14-3), la fecha y hora, y una descripción del suceso.

3. Haga clic en el botón correspondiente de la página **Registro de sucesos del sistema** para continuar (consulte la tabla 14-4).

Tabla 14-4. Botones de la página del registro de sucesos del sistema

Botón	Acción
Imprimir	Imprime el **registro de sucesos del sistema en el orden en que aparece en la ventana.**
Borrar registro	Borra el **registro de sucesos del sistema**. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso para **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **registro de sucesos del sistema** en el directorio de su elección. **NOTA:** Si va a usar Internet Explorer y encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft® en support.microsoft.com.
Actualizar	Vuelve a cargar la página **Registro de sucesos del sistema**.

Consulta de los códigos POST

La página **Códigos POST** muestra el último código de la autoprueba de encendido del sistema antes de iniciar el sistema operativo. Los códigos POST son indicadores de progreso del sistema BIOS que indican varias etapas de la secuencia de inicio desde el restablecimiento de la alimentación, y que permiten diagnosticar fallas relativas al inicio del sistema.

NOTA: Vea el texto para conocer los números de mensaje de códigos POST en la pantalla LCD o en el *Manual del propietario del hardware*.

Para ver los códigos POST, realice los pasos siguientes:

1. Haga clic en **Sistema**, en la ficha **Registros** y después en **Códigos POST**.

   La página **Códigos POST** muestra un indicador de condición del sistema (consulte la tabla 14-3), un código hexadecimal y una descripción del código.

2. Haga clic en el botón correspondiente de la página **Código POST** para continuar (consulte la tabla 14-5).

Tabla 14-5. Botones de códigos POST

Botón	Acción
Imprimir	Imprime la página **Códigos POST**.
Actualizar	Vuelve a cargar la página **Códigos POST**.

Visualización de la pantalla de último bloqueo del sistema

AVISO: La función de pantalla de último bloqueo se debe configurar en Server Administrator y en la interfaz web del iDRAC. Consulte Configuración del servidor administrado para capturar la pantalla de último bloqueo para obtener instrucciones sobre cómo configurar esta función.

La página **Pantalla de último bloqueo** muestra la pantalla del bloqueo más reciente, que incluye información sobre los sucesos que ocurrieron antes de que el sistema se bloqueara. La imagen del último bloqueo del sistema se guarda en la memoria permanente del iDRAC y se puede acceder a ella de manera remota.

Para ver la página **Pantalla de último bloqueo**, realice los pasos a continuación:

- Haga clic en la ficha **Sistema**, en la ficha **Registros** y luego haga clic en **Último bloqueo**.

La página **Pantalla de último bloqueo** tiene los botones que se muestran en la tabla 14-6:

NOTA: Los botones **Guardar** y **Eliminar** no aparecerán si no hay ninguna pantalla de bloqueo guardada.

Tabla 14-6. Botones de la página Pantalla de último bloqueo

Botón	Acción
Imprimir	Imprime la página **Pantalla de último bloqueo**.
Guardar	Abre una ventana emergente que le permite guardar la página **Pantalla de último bloqueo** en un directorio de su elección.
Eliminar	Elimina la página **Pantalla de último bloqueo**.
Actualizar	Vuelve a cargar la página **Pantalla de último bloqueo**.

NOTA: Debido a fluctuaciones en el temporizador de la recuperación automática, es posible que la **Pantalla de último bloqueo** no pueda capturarse cuando el temporizador de restablecimiento del sistema tenga un valor demasiado alto. El valor predeterminado es de 480 segundos. Utilice Server Administrator o IT Assistant para definir el temporizador de restablecimiento del sistema como 60 segundos y para asegurarse de que la **Pantalla de último bloqueo** funcione correctamente. Consulte Configuración del servidor administrado para capturar la pantalla de último bloqueo para obtener más información.

Visualización de las secuencias de inicio más recientes

Si experimenta problemas de inicio, puede ver la actividad de pantalla de lo que ha sucedido durante las últimas tres secuencias de inicio de la página Captura de inicio. La reproducción de las pantallas de inicio ocurre a una velocidad de 1 marco por segundo. La tabla 14-7 presenta una lista de las acciones de control disponibles.

NOTA: Debe disponer de privilegios de administrador para ver la reproducción de las secuencias de Captura de inicio.

Tabla 14-7. Opciones de Captura de inicio

Botón/Opción	Descripción
Selecciona la secuencia de inicio	Permite seleccionar la secuencia de inicio para cargar y reproducir. - Captura de inicio 1: carga la secuencia de inicio más reciente. - Captura de inicio 2: carga la secuencia de inicio (segunda más reciente) que ocurrió antes de la Captura de inicio 1. - Captura de inicio 3: carga la secuencia de inicio (tercera más reciente) que ocurrió antes de la Captura de inicio 2.
Guardar como	Crea un archivo .zip comprimido que contiene todas las imágenes de captura de inicio de la secuencia actual. El usuario debe disponer de privilegios de administración para realizar esta acción.
Pantalla anterior	Lo lleva a la pantalla anterior, de existir, en la consola de reproducción.
Reproducir	Inicia la reproducción de la pantalla actual en la consola de reproducción.
Pausa	Interrumpe la reproducción en la pantalla actual que se está mostrando en la consola de reproducción.
Stop	Detiene la reproducción de pantalla y carga la primera pantalla de esa secuencia de inicio.
Próxima pantalla	Lo lleva a la pantalla siguiente, de existir, en la consola de reproducción.
Imprimir	Imprime la imagen de Captura de inicio que aparece en la pantalla.
Actualizar	Vuelve a cargar la página de Captura de inicio.

Consulta de la pantalla de estado del sistema en busca de mensajes de error

Cuando un indicador LED parpadea en color ámbar y un servidor específico tiene un error, la pantalla de estado del servidor en la pantalla LCD resaltará el servidor afectado con un color naranja. Use los botones de navegación de la pantalla LCD para resaltar el servidor afectado y después haga clic en el botón central. Los mensajes de error y advertencia aparecerán en la segunda línea. La tabla siguiente muestra una lista de todos los mensajes de error y la gravedad de los mismos.

Tabla 14-8. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Advertencia	Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de advertencia	La temperatura ambiental del servidor superó el umbral de advertencia
Crítico	Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de falla	La temperatura ambiental del servidor superó el umbral de falla
Crítico	Batería CMOS de la placa del sistema: sensor de la batería de la placa del sistema, se confirmó una falla	No hay batería CMOS o no tiene carga
Advertencia	Nivel de sistema de la placa del sistema: sensor de corriente de la placa del sistema, suceso de advertencia	La corriente superó un umbral de advertencia
Crítico	Nivel de sistema de la placa del sistema: sensor de corriente de la placa del sistema, suceso de falla	La corriente superó un umbral de falla
Crítico	CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la CPU<número>, se confirmó el estado declarado	Voltaje fuera de rango
Crítico	<Nombre del sensor de voltaje> de la placa del sistema: sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Voltaje fuera de rango
Crítico	CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la CPU<número>, se confirmó el estado declarado	Voltaje fuera de rango
Crítico	Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó IERR	Falla de la CPU
Crítico	Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó un disparo térmico	La CPU se sobrecalentó
Crítico	Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó un error de configuración	Tipo incorrecto de procesador o instalación en el lugar erróneo
Crítico	Estado de la CPU<número>: sensor de procesador de la CPU<número>, no se confirmó la presencia	La CPU requerida falta o no está presente
Crítico	Tarjeta vertical de vídeo de la placa del sistema: sensor de módulo de la placa del sistema, se confirmó el retiro del dispositivo	Se retiró el módulo requerido
Crítico	Estado de la tarjeta intermediaria B<número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria B<número de ranura>, se confirmó un error de instalación	Se instaló una tarjeta intermediaria incorrecta para la red Fabric de E/S
Crítico	Estado de la tarjeta intermediaria C<número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria C<número de ranura>, se confirmó un error de instalación	Se instaló una tarjeta intermediaria incorrecta para la red Fabric de E/S
Crítico	Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se retiró la unidad	Se retiró la unidad de almacenamiento
Crítico	Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se confirmó una falla de la unidad	Falló la unidad de almacenamiento
Crítico	Protección contra fallas PFault de la placa del sistema: sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Este suceso se genera cuando los voltajes de la placa del sistema no se encuentran en los niveles normales.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó que el temporizador ha expirado	El temporizador de la vigilancia de iDRAC expiró y no se estableció ninguna acción.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó un reinicio	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de reiniciar.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó el apagado	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de apagado.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó un ciclo de encendido	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de ciclo de encendido.
Crítico	Registro de sucesos de la placa del sistema: sensor de registro de sucesos de la placa del sistema, se confirmó que el registro está lleno	El dispositivo de registro de sucesos del sistema detecta que sólo se podrá agregar una anotación al registro antes de que se llene.
Advertencia	Error corregible de ECC: sensor de memoria, se confirmó un ECC corregible (<ubicación del DIMM>)	Los errores ECC corregibles alcanzaron una frecuencia crítica.
Crítico	Error incorregible de ECC: se confirmó un ECC incorregible (<ubicación del DIMM>) se confirmó	Se detectó un error ECC incorregible.
Crítico	Rev. de canal de E/S: sensor de sucesos críticos, se confirmó una NMI?de revisión de canal de E/S	Se genera una interrupción crítica en el canal de E/S.
Crítico	Error de paridad de PCI: sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de paridad en el bus PCI.
Crítico	Error de sistema de PCI: sensor de sucesos críticos, se confirmó un SERR de PCI (<número de ranura o id. de dispositivo PCI>)	El dispositivo detectó un error de PCI
Crítico	Registro SBE desactivado: sensor de registro de sucesos, se confirmó la desactivación del registro de errores corregibles de memoria	El registro de errores de un solo bit se desactiva cuando se registran demasiados SBE (errores de un solo bit)
Crítico	Desactivación de registro: sensor del registro de sucesos, se confirmó la desactivación de todo registro de sucesos	Se desactivó todo registro de errores
No recuperable	Error de protocolo de CPU: sensor de procesador, se confirmó la transición a estado no recuperable	El protocolo del procesador ingresó a un estado no recuperable.
No recuperable	PERR de bus de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	El PERR de bus del procesador ingresó a un estado no recuperable.
No recuperable	Error de inicialización de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	La inicialización del procesador ingresó a un estado no recuperable.

No recuperable	Revisión de máquina de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	La revisión de máquina del procesador ingresó a un estado no recuperable.
Crítico	Repuesto de memoria: sensor de memoria, se confirmó la pérdida de la redundancia (<ubicación del DIMM>) se confirmó	El repuesto de la memoria ya no es redundante.
Crítico	Memoria reflejada: sensor de memoria, se confirmó la pérdida de la redundancia (<ubicación del DIMM>) se confirmó	La memoria reflejada ya no es redundante
Crítico	RAID de memoria: sensor de memoria, se confirmó la pérdida de redundancia (<ubicación del DIMM>)	La memoria de RAID ya no es redundante
Advertencia	Se agregó memoria: sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria agregado.
Advertencia	Se quitó la memoria: sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se quitó el módulo de memoria.
Crítico	Error de configuración de memoria: sensor de memoria, se confirmó un error de configuración (<ubicación del DIMM>) se confirmó	La configuración de la memoria no es correcta para el sistema.
Advertencia	Ganancia de redundancia de memoria: sensor de memoria, la degradación de la redundancia (<ubicación del DIMM>) se confirmó	La redundancia de la memoria se ha degradado pero no se ha perdido
Crítico	Error fatal de PCIE: sensor de sucesos críticos, se confirmó un error fatal de bus	Se detectó un error fatal en el bus de PCIE.
Crítico	Error de chipset: sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de chip.
Advertencia	Advertencia de memoria ECC: sensor de memoria, se confirmó la transición de buen estado a estado no crítico (<ubicación del DIMM>)	Los errores corregibles ECC han aumentado por encima de la frecuencia normal.
Crítico	Advertencia de memoria ECC: sensor de memoria, se confirmó la transición de un estado crítico a uno menos grave (<ubicación del DIMM>)	Los errores ECC corregibles han alcanzado una frecuencia crítica.
Crítico	Error de la POST: sensor de la POST, no hay memoria instalada	No se detectó memoria en la placa
Crítico	Error de la POST: sensor de la POST, error de configuración de memoria	Se ha detectado la memoria, pero no se puede configurar
Crítico	Error de la POST: sensor de la POST, error de memoria inutilizable	Se ha configurado la memoria, pero no se puede utilizar
Crítico	Error de la POST: sensor de la POST, falló el copiado del BIOS en la RAM	Falla de copiado de BIOS en la RAM?del sistema
Crítico	Error de la POST: sensor de la POST, falló el CMOS	Error de CMOS
Crítico	Error de la POST: sensor de la POST, falló el controlador de DMA	Error del controlador de DMA
Crítico	Error de la POST: sensor de la POST, falló el controlador de interrupción	Error del controlador de interrupción
Crítico	Error de la POST: sensor de la POST, falló la actualización del temporizador	Error de actualización del temporizador
Crítico	Error de la POST: sensor de la POST, error de temporizador de intervalos programable	Error del temporizador de intervalos programable
Crítico	Error de la POST: sensor de la POST, error de paridad	Error de paridad
Crítico	Error de la POST: sensor de la POST, falló el SIO	Error de SIO
Crítico	Error de la POST: sensor de la POST, falló el controlador de teclado	Falla del controlador del teclado
Crítico	Error de la POST: sensor de la POST, falló la inicialización de interrupción de administración del sistema	Error de inicialización en la interrupción de administración del sistema
Crítico	Error de la POST: sensor de la POST, falló la prueba de apagado del BIOS	Error de la prueba de apagado del BIOS
Crítico	Error de la POST: sensor de la POST, falló la prueba de memoria del BIOS durante la POST	Error de la prueba de la memoria del BIOS durante la POST
Crítico	Error de la POST: sensor de la POST, falló la configuración de Dell Remote Access Controller	Error de configuración de Dell Remote Access Controller
Crítico	Error de la POST: sensor de la POST, falló la configuración de la CPU	Error de configuración de la CPU
Crítico	Error de la POST: sensor de la POST, configuración incorrecta de la memoria	Configuración incorrecta de la memoria
Crítico	Error de la POST: sensor de la POST, falló la POST	Error general tras el vídeo
Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware	Se detectó hardware incompatible
Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware (firmware del BMC)	El hardware es incompatible con el firmware
Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware (incorrespondencia entre la CPU y el firmware del BMC)	La CPU y el firmware no son compatibles
Crítico	Sobrecalentamiento de memoria: sensor de memoria, se confirmó un ECC corregible <ubicación del DIMM>	Sobrecalentamiento del módulo de memoria
Crítico	CRC fatal de SB de memoria: sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Sur
Crítico	CRC fatal de NB de memoria: sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Norte
Crítico	Temporizador de vigilancia: sensor de vigilancia, se confirmó el reinicio	El temporizador de vigilancia hizo que el sistema se reiniciara
Crítico	Temporizador de vigilancia: sensor de vigilancia, se confirmó la expiración del temporizador	El temporizador de vigilancia expiró pero no se realizó ninguna acción
Advertencia	Ajuste de vínculo: sensor de cambios de versión, no se confirmó un cambio satisfactorio de software ni firmware	No se pudo actualizar el valor de ajuste de vínculo para lograr un funcionamiento adecuado del NIC

Advertencia	Ajuste de vínculo: sensor de cambios de versión, no se confirmó el cambio satisfactorio de hardware <número de ranura del dispositivo>	No se pudo actualizar el valor de ajuste de vínculo para lograr un funcionamiento adecuado del NIC
Crítico	FlexAddr/Link: sensor de ajuste de vínculo, se confirmó el error de programación de la dirección MAC?virtual (nº de bus, nº. de dispositivo, nº. de función)	No se pudo programar la dirección flexible para este dispositivo
Crítico	FlexAddr/Link: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción para apoyar el ajuste de vínculo o la dirección flexible (tarjeta intermediaria <ubicación>)	La ROM?de opción no admite la dirección flexible ni el ajuste de vinculación.
Crítico	FlexAddr/Link: sensor de ajuste de vínculo, se confirmó un error para obtener datos de ajuste de vínculo o de FlexAddress del BMC/iDRAC	No se pudo obtener información de ajuste de vinculación ni FlexAddress del BMC/iDRAC
Crítico	FlexAddr/Link: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción para apoyar el ajuste de vínculo o FlexAddress (tarjeta intermediaria XX)	Este evento se genera cuando la opción ROM del dispositivo PCI para una NIC no es compatible con la función de ajuste de vínculo o FlexAddress.
Crítico	FlexAddr/Link: sensor de ajuste de vínculo, se confirmó un error en la programación de la dirección MAC virtual (<ubicación>)	Este evento se genera cuando el BIOS no puede programar la dirección MAC virtual en un dispositivo NIC específico.
Crítico	Error fatal E/S: sensor de grupo ES fatal, error ES fatal (<ubicación>)	Este evento se genera en relación con un IERR de CPU e indica qué dispositivo causó el IERR de CPU.
Advertencia	Error no fatal PCIE: sensor de grupo E/S no fatal, error PCIe (<ubicación>)	Este evento se genera en relación con un IERR de CPU.

Visualización del registro del iDRAC

El **Registro del iDRAC** es un registro persistente que se mantiene en el firmware de iDRAC. El registro contiene una lista de las acciones de usuario (como inicio y cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC. Cuando el registro se llena, las anotaciones más antiguas se sobrescriben.

El **Registro de sucesos del sistema** (SEL) contiene anotaciones de sucesos que ocurren en el servidor administrado y el **Registro del iDRAC** contiene anotaciones de sucesos que ocurren en el iDRAC.

Para acceder al registro del **iDRAC**, realice los pasos siguientes:

- Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y después haga clic en **Registro del iDRAC**.

El **Registro del iDRAC** proporciona la información que aparece en la tabla 14-9.

Tabla 14-9. Información de la página del registro del iDRAC

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 de dic. 16:55:47). El iDRAC obtiene la hora del reloj del servidor administrado. Cuando el iDRAC se inicie y no pueda comunicarse con el servidor administrado, la hora aparecerá como cadena de 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 iDRAC.

Uso de los botones de la página de registro del iDRAC

La página **Registro del iDRAC** tiene los siguientes botones (consulte la tabla 14-10).

Tabla 14-10. Botones del registro del iDRAC

Botón	Acción
Imprimir	Imprime la página **Registro del iDRAC**.
Borrar registro	Borra las anotaciones del **Registro del iDRAC**. **NOTA:** El botón **Borrar registro** sólo aparecerá si usted tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **Registro del iDRAC** en un directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en **support.microsoft.com**.
Actualizar	Vuelve a cargar la página **Registro del iDRAC**.

Cómo ver la información del sistema

La página **Resumen del sistema** muestra la información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller

Para acceder a la información del sistema, haga clic en **Sistema**→ **Propiedades**.

Gabinete del sistema principal

La tabla 14-11 y la tabla 14-12 describen las propiedades del chasis de sistema principal.

Tabla 14-11. Campos de la información del sistema

Campo	Descripción
Descripción	Proporciona una descripción del sistema.
Versión del BIOS	Muestra la versión del BIOS del sistema.
Etiqueta de servicio	Muestra el número de la etiqueta de servicio del sistema.
Nombre del host	Proporciona el nombre del sistema host.
Nombre del sistema operativo	Muestra el sistema operativo que se ejecuta en el sistema.

Tabla 14-12. Campos de la recuperación automática

Campo	Descripción
Acción de recuperación	Cuando se detecta un *bloqueo de sistema*, el iDRAC se puede configurar para que ejecute una de las acciones siguientes: **Sin acción**, **Restablecimiento forzado**, **Apagar** o **Ciclo de encendido**.
Cuenta regresiva inicial	El número de segundos después que se detecta un *bloqueo de sistema* al término de los cuales el iDRAC ejecutará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Integrated Dell Remote Access Controller

La tabla 14-13 describe las propiedades del iDRAC.

Tabla 14-13. Campos informativos del iDRAC

Campo	Descripción
Fecha/Hora	Proporciona la fecha y hora actuales en el iDRAC en el formato de hora media de Greenwich.
Versión del firmware	Enumera la versión del firmware del iDRAC.
Firmware actualizado	Enumera la fecha en la que el firmware se ha actualizado por última vez. La fecha se muestra en formato UTC, por ejemplo: Jue, 8 de mayo de 2007, 22:18:21 UTC.
Dirección IP	La dirección de 32 bits que identifica la interfaz de red. El valor se muestra en formato de *números separados con puntos*, por ejemplo, 143.166.154.127.
Puerta de enlace	La dirección IP de la puerta de enlace que actúa como vínculo a otras redes. Este valor está en formato de *números separados con puntos*, por ejemplo, 143.166.150.5.
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.
Dirección MAC	La dirección de Control de acceso a medios (MAC) que identifica de manera exclusiva a cada NIC en una red, por ejemplo: 00-00-0c-ac-08. Ésta es una identificación asignada por Dell y no se puede modificar.
DHCP activado	**Activado** indica que el protocolo de configuración dinámica de host (DHCP) está activado. **Desactivado** indica que DHCP *no* está activado.

Identificación del servidor administrado en el chasis

El chasis PowerEdge M1000e alberga hasta dieciséis servidores. Para localizar a un servidor específico en el chasis, puede usar la interfaz web del iDRAC para activar un parpadeo del LED del servidor en color azul. Cuando active el LED, puede especificar el número de segundos que desea que el LED parpadee para asegurarse que podrá localizar el chasis mientras el LED aún esté parpadeando. Si introduce 0, el LED parpadeará hasta que usted lo desactive.

Para identificar el servidor:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Solución de problemas**.
2. En la página **Identificar**, seleccione el cuadro junto a **Identificar el servidor**.
3. En el campo **Tiempo de espera para identificar el servidor**, introduzca el número de segundos que desea que el LED parpadee. Introduzca 0 si desea que el LED siga parpadeando hasta que usted lo desactive.
4. Haga clic en **Aplicar**.

El LED del servidor parpadeará en color azul durante el número de segundos que usted haya especificado.

Si introduce 0 para dejar el LED parpadeando, siga estos pasos para desactivarlo:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Solución de problemas**.
2. En la página **Identificar**, deseleccione el cuadro que se encuentra junto a **Identificar el servidor**.
3. Haga clic en **Aplicar**.

Uso de la consola de diagnósticos

El iDRAC proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la tabla 14-14) que son similares a las herramientas que se incluyen con los sistemas con Microsoft® Windows® o Linux. Por medio de la interfaz web de iDRAC, se puede acceder a las herramientas de depuración de red.

Para tener acceso a la página **Consola de diagnósticos**, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **iDRAC**→ **Solución de problemas**.
2. Haga clic en la ficha **Diagnósticos**.

La tabla 14-14 describe los comandos que se pueden introducir en la página **Consola de diagnósticos**. Escriba un comando y haga clic en **Enviar**. Los resultados de depuración aparecerán en la página **Consola de diagnósticos**.

Haga clic en el botón **Borrar** para borrar los resultados generados por el comando anterior.

Para actualizar la página **Consola de diagnósticos**, haga clic en **Actualizar**.

Tabla 14-14. 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.
ping *<Dirección IP>*	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo de iDRAC. Para obtener más información, consulte el apartado gettracelog.

Administración de alimentación en un sistema remoto

El iDRAC permite realizar de manera remota varias acciones de administración de alimentación en el servidor administrado. Use la página Administración de la alimentación para realizar un apagado ordenado por medio del sistema operativo al reiniciar, encender y apagar el sistema.

NOTA: Debe tener permiso para **Ejecutar comandos de acción de servidor** para realizar acciones de administración de alimentación. Consulte Cómo agregar y configurar usuarios de iDRAC para obtener ayuda con la configuración de permisos de usuario.

1. Haga clic en **Sistema** y después haga clic en la ficha **Administración de la alimentación**.
2. Seleccione una **Acción de control de alimentación**, por ejemplo, **Restablecer el sistema (reinicio mediante sistema operativo)**. La tabla 14-15 contiene información sobre las acciones de control de alimentación.
3. Haga clic en **Aplicar** para realizar la acción seleccionada.
4. Para continuar, haga clic en el botón correspondiente. Consulte el apartado tabla 14-16.

Tabla 14-15. Acciones de control de alimentación

Encender el sistema	Enciende la alimentación del sistema (equivalente a oprimir el botón de encendido cuando el sistema está apagado).
Apagar el sistema	Apaga la alimentación del sistema (equivalente a oprimir el botón de encendido cuando el sistema encendido).
NMI (Interrupción no enmascarable)	Envía una interrupción de alto nivel al sistema operativo, lo cual hace que el sistema detenga la operación para permitir actividades fundamentales de diagnóstico o solución de problemas.
Apagado ordenado	Intenta cerrar de manera estructurada el sistema operativo y luego apaga el sistema. Requiere un sistema operativo con ACPI (Interfaz de energía y configuración avanzada), lo cual permite que el sistema dirija la administración de la alimentación.
Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo (reinicio mediante sistema operativo).
Realizar ciclo de encendido del sistema	Apaga el sistema y después lo reinicia (reinicio mediante suministro de energía).

Tabla 14-16. Botones de página de administración de la alimentación

Botón	Acción
Imprimir	Imprime los valores de la **Administración de la alimentación** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Administración de la alimentación**.
Aplicar	Guarda cualquier configuración nueva que asigne mientras esté en la página Administración de la alimentación.

Solución de problemas y preguntas frecuentes

La tabla 14-17 contiene la preguntas frecuentes sobre problemas de solución de problemas.

Tabla 14-17. Preguntas frecuentes/solución de problemas

Pregunta	Respuesta
El indicador LED del servidor parpadea en color ámbar.	Revise el registro de sucesos del sistema en busca de mensajes y después bórrelo para detener el parpadeo del indicador LED. En la interfaz web del iDRAC: • Consulte el apartado Consulta del registro de sucesos del sistema (SEL). En SM-CLP: • Consulte el apartado Administración del registro de sucesos del sistema. En la utilidad de configuración del iDRAC: • Consulte el apartado Menú del registro de sucesos del sistema.
Hay un LED que parpadea de color azul en el servidor.	Un usuario ha activado la identificación de localizador del servidor. Ésta es una señal para ayudar a identificar el servidor en el chasis. Consulte Identificación del servidor administrado en el chasis para obtener información sobre esta función.
¿Cómo puedo encontrar la dirección IP del iDRAC?	En la interfaz web del CMC: 1. Haga clic en **Chasis**→ **Servidores** y después haga clic en la ficha **Configuración**. 2. Haga clic en **Instalar**. 3. Lea la dirección IP del servidor en la tabla que aparece. En el iKVM: • Reinicie al servidor e introduzca la utilidad de configuración del iDRAC presionando <Ctrl><E> O bien: • Espere a que la dirección IP aparezca durante la POST del BIOS. O bien: • Seleccione la consola "Dell CMC" en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía del usuario del firmware del CMC* para una lista completa de los subcomandos RACADM del CMC.
¿Cómo puedo encontrar la dirección IP del iDRAC? *(continuación)*	Por ejemplo: $ racadm getniccfg -m server-1 DHCP activado = 1 Dirección IP = 192.168.0.1 Máscara de subred = 255.255.255.0

	Puerta de enlace = 192.168.0.1 En RACADM local: 1. Introduzca el comando siguiente en una petición de comandos: racadm getsysinfo En la pantalla LCD: 1. En el menú principal, marque **Servidor** y presione el botón de verificación. 2. Seleccione el servidor cuya dirección IP busca y presione el botón de verificación.
¿Cómo puedo encontrar la dirección IP del CMC?	En la interfaz web del iDRAC: l Haga clic en **Sistema**→ **Acceso remoto**→ **CMC**. La dirección IP del CMC se muestra en la página **Resumen**. O bien: l Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía del usuario del firmware del CMC* para una lista completa de los subcomandos RACADM del CMC. $ racadm getniccfg -m chassis NIC activado = 1 DHCP activado = 1 Dirección IP estática = 192.168.0.120 Máscara de subred estática = 255.255.255.0 Puerta de enlace estática = 192.168.0.1 Dirección IP actual = 10.35.155.151 Máscara de subred actual = 255.255.255.0 Puerta de enlace actual = 10.35.155.1 Velocidad = Negociación automática Dúplex = Negociación automática
La conexión de red del iDRAC no funciona.	l Asegúrese de que el cable de la LAN esté conectado con el CMC. l Asegúrese de que la LAN del iDRAC esté activada.
Inserté el servidor en el chasis y presioné el botón de encendido, pero no pasó nada.	l El iDRAC requiere de alrededor de 30 segundos para inicializarse antes de que el servidor se pueda encender. Espere durante 30 segundos y luego presione el botón de encendido otra vez. l Revise el presupuesto de alimentación del CMC. Es posible que el presupuesto de alimentación del chasis se haya excedido.
Olvidé el nombre del usuario administrativo del iDRAC y la contraseña.	Deberá restaurar los valores predeterminados del iDRAC. 1. Reinicie al servidor y presione <Ctrl><E> cuando se le solicite para ingresar a la utilidad de configuración del iDRAC. 2. En el menú de la utilidad de configuración, marque **Restablecer los valores predeterminados** y presione <Entrar>. Para obtener más información, consulte Restablecer valores predeterminados.
¿Cómo puedo cambiar el nombre de la ranura de mi servidor?	1. Inicie sesión en la interfaz web del CMC. 2. Abra el árbol **Chasis** y haga clic en **Servidores**. 3. Haga clic en la ficha **Configuración**. 4. Escriba el nuevo nombre para la ranura en la fila del servidor. 5. Haga clic en **Aplicar**.
Cuando se inicie una sesión de redirección de consola en la interfaz web del iDRAC, aparecerá una ventana emergente de seguridad de ActiveX.	Es posible que el iDRAC no sea un sitio de confianza en el explorador de cliente. Para evitar que la ventana emergente de seguridad aparezca cada vez que usted comience una sesión de redirección de consola, agregue el iDRAC a la lista de sitios de confianza: 1. Haga clic en **Herramientas**→ **Opciones de Internet...**→ **Seguridad**→ **Sitios de confianza**. 2. Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS del iDRAC. 3. Haga clic en **Agregar**.
Cuando inicio una sesión de redirección de consola, la pantalla del visor está en blanco.	Si usted tiene privilegio de **Medios virtuales**, pero no privilegio de **Redirección de consola**, podrá iniciar el visor para que pueda acceder a la función de medios virtuales, pero la consola del servidor administrado no aparecerá.
El iDRAC no se inicia.	Retire el servidor e insértelo nuevamente. Revise la interfaz web del CMC para ver si el iDRAC aparece como componente que se puede actualizar. Si lo hace, siga las instrucciones de la sección Recuperación del firmware del iDRAC por medio del CMC. Si esto no corrige el problema, póngase en contacto con el personal de asistencia técnica.
Cuando trato de iniciar el servidor administrado, el indicador de alimentación es de color verde, pero no hay POST ni vídeo.	Esto puede pasar si se presenta cualquiera de las condiciones siguientes: l La memoria no está instalada o no se puede acceder a ella. l La CPU no está instalada o no se puede tener acceso a ella. l La tarjeta de vídeo está ausente o no está conectada correctamente. Asimismo, busque mensajes de error en el registro del iDRAC desde la interfaz web del iDRAC o en la pantalla LCD.

Regresar a la página de contenido

Regresar a la página de contenido

Glosario

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Active Directory

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

ARP

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

ASCII

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

BIOS

Siglas de basic input/output system (sistema básico de entradas y salidas), que es la parte del software de sistema que proporciona la interfaz al nivel más bajo a los dispositivos periféricos y que controla la primera fase del proceso de inicio del sistema, incluyendo la instalación del sistema operativo en la memoria.

bus:

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

CA

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

captura SNMP

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

CD

Siglas de compact disc (disco compacto).

CHAP

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

CIM

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

CLI

Siglas de command-line interface (interfaz de línea de comandos).

CLP

Siglas de command-line protocol (protocolo de línea de comandos).

CSR

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

DDNS

Siglas de Dynamic Domain Name System (Sistema de nombres de dominio dinámicos).

DHCP

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

Dirección MAC

Abreviatura para dirección "media access control" (control de acceso a medios), que es una dirección única incorporada en los componentes físicos de una NIC.

disco RAM

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

DLL

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

DMTF

Siglas de Distributed Management Task Force (Equipo de trabajo de administración distribuida).

DNS

Siglas de Domain Name System (Sistema de nombres de dominio).

DSU

Abreviatura de disk storage unit (unidad de almacenamiento en disco).

esquema ampliado

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

esquema estándar

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

Estación de administración

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

FQDN

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

FSMO

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

GMT

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

GPIO

Abreviatura de general purpose input/output (entrada/salida de propósito general).

GRUB

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

GUI

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

hardware log

Registra los sucesos generados por el iDRAC6.

iAMT

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

ICMB

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

ICMP

Siglas de Internet control message protocol (protocolo de mensajes de control de Internet).

ID

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

iDRAC6

Siglas de Integrated Dell Remote Access Controller, el sistema de supervisión y control integrado en el chip de los servidores Dell 11G PowerEdge.

IP

Abreviatura de Internet Protocol (protocolo de Internet), que es un nivel de red de TCP/IP. El IP proporciona enrutamiento, fragmentación y reensamblaje de paquetes.

IPMB

Siglas de intelligent platform management bus (bus de administración de plataforma inteligente), que es un bus que se utiliza en la tecnología de administración de sistemas.

IPMI

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

Kbps

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

LAN

Abreviatura de local area network (red de área local).

LDAP

Abreviatura de protocolo ligero de acceso a directorios.

LED

Abreviatura de diodo emisor de luz.

LOM

Abreviatura de local area network on motherboard (red de área local integrada a la placa base).

LUN

Siglas del número de unidad lógica.

MAC

Siglas de media access control (control de acceso a medios), que es un subnivel de red entre un nodo de red y el nivel físico de la red.

MAP

Siglas de Manageability Access Point (Punto de acceso de administrabilidad).

Mbps

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

MIB

Abreviatura de management information base (base de información de administración).

MII

Siglas de Media Independent Interface (Interfaz independiente de medios).

NAS

Abreviatura de network attached storage (almacenamiento conectado a red).

NIC

Siglas de network interface card (tarjeta de interfaz de red). Una placa adaptadora de circuitos instalada en un equipo para brindar una conexión física con la red.

OID

Abreviatura de Object Identifiers (identificadores de objeto).

PCI

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

POST

Siglas de power-on self-test (autoprueba de encendido), que es una secuencia de pruebas de diagnóstico que un sistema ejecuta automáticamente cuando se enciende.

PPP

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

RAC

Abreviatura de remote access controller (controlador de acceso remoto).

RAM

Siglas de memoria de acceso aleatorio. La RAM es una memoria de propósito general que se puede leer y en la que se puede escribir en los sistemas y en el iDRAC6.

redirección de consola

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

reversión

Para revertir a una versión anterior de software o firmware.

ROM

Siglas de read-only memory (memoria de sólo lectura), que es la memoria desde la cual es posible leer los datos, pero no se pueden escribir en ella.

RPM

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

SAC

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

SAI

Abreviatura de sistema de energía ininterrumpida.

SAP

Siglas de Service Access Point (Punto de acceso de servicio).

SEL

Siglas de registro de sucesos del sistema.

servidor administrado

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

sistema administrado

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

SM-CLP

Abreviación de protocolo de línea de comandos de administrador de servidor. SM-CLP es un subcomponente de la iniciativa de SMASH supervisado por DMTF para una administración efectiva del servidor a lo largo de varias plataformas. La especificación SM-CLP, junto con la especificación de dirección del elemento administrado y los numerosos perfiles para las especificaciones de asignación de SM-CLP, describe los verbos y los objetivos estandarizados para la ejecución de varias tareas de administración.

SMI

Abreviatura de systems management interrupt (interrupción de administración del sistema).

SMTP

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

SMWG

Siglas de Systems Management Working Group (Grupo de trabajo de administración de sistemas).

SSH

Abreviatura para Secure SHell.

SSL

Abreviatura de secure sockets layer (capa de conexión segura).

TAP

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

TCP/IP

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

TFTP

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

Unified Server Configurator

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

USB

Abreviatura de bus serial universal.

USC

Abreviación de Unified Server Configurator.

UTC

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

VLAN

Siglas de Virtual Local Area Network (Red virtual de área local).

VNC

Abreviatura de virtual network computing (cómputo de red virtual).

VT-100

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

WAN

Abreviatura de wide area network (red de área amplia).

WS-MAN

Abreviación del protocolo de servicios web para administración (WS-MAN:Web Services for Management). WS-MAN es un mecanismo de transporte para el intercambio de información. WS-MAN brinda un idioma universal para que los dispositivos compartan datos a fin de que puedan administrarse con más facilidad.

Regresar a la página de contenido

Regresar a la página de contenido

Generalidades del subcomando RACADM

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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

---

help

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

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

Tabla A-1. Comando help

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

Sinopsis

```
racadm help

racadm help <subcomando>
```

Descripción

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

Salida

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

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

Interfaces admitidas

- RACADM local
- RACADM remota

- RACADM Telnet/SSH/serie

---

arp

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

En la Tabla A-2 se describe el comando **arp**.

Tabla A-2. Comando arp

Comando	Definición
arp	Muestra el contenido de la tabla de ARP. Las anotaciones del ARP no se pueden agregar ni eliminar.

Sinopsis

```
racadm arp
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

clearasrscreen

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

En la Tabla A-3 se describe el subcomando **clearasrscreen**.

Tabla A-3. clearasrscreen

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

Sinopsis

```
racadm clearasrscreen
```

Interfaces admitidas

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

---

config

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

En la Tabla A-4 se describen los subcomandos **config** y **getconfig**.

Tabla A-4. config/getconfig

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

Sinopsis

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

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

Interfaces admitidas

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

Descripción

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

Entrada

En la Tabla A-5 se describen las opciones del subcomando **config**.

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

Tabla A-5. Opciones y descripciones del subcomando config

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

Salida

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

- Sintaxis, nombre de grupo, nombre de objeto o índice no válidos, u otros miembros no válidos de la base de datos
- Fallas de la CLI de RACADM

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

Ejemplos

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

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

- `racadm config -f myrac.cfg`

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

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

---

getconfig

Descripción del subcomando getconfig

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

Entrada

En la Tabla A-6 se describen las opciones del subcomando **getconfig**.

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

Tabla A-6. Opciones del subcomando getconfig

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

Salida

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

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

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

Ejemplos

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

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

- `racadm getconfig -h`

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

- `racadm getconfig -u root`

Muestra las propiedades de configuración del usuario root.

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

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

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>

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

racadm getconfig -u <nombre_de_usuario>

racadm getconfig -h
```

Interfaces admitidas

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

---

coredump

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

En la Tabla A-7 se describe el subcomando **coredump**.

Tabla A-7. coredump

Subcomando	Definición
coredump	Muestra el último volcado central del iDRAC6.

Sinopsis

```
racadm coredump
```

Descripción

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

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

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

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

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

coredumpdelete

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

En la Tabla A-8 se describe el subcomando **coredumpdelete**.

Tabla A-8. coredumpdelete

Subcomando	Definición
coredumpdelete	Borra el volcado central almacenado en el iDRAC6.

Sinopsis

```
racadm coredumpdelete
```

Descripción

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

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

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

Interfaces admitidas

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

---

fwupdate

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

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

En la Tabla A-9 se describe el subcomando **fwupdate**.

Tabla A-9. fwupdate

Subcomando	Definición
fwupdate	Actualiza el firmware del iDRAC6

Sinopsis

```
racadm fwupdate -s

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

racadm fwupdate -r
```

Descripción

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

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

Interfaces admitidas

- RACADM local
- RACADM Telnet/SSH/serie

Entrada

En la Tabla A-10 se describen las opciones del subcomando **fwupdate**.

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

Tabla A-10. Opciones del subcomando fwupdate

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

Salida

Muestra un mensaje que indica qué operación se está ejecutando.

Ejemplos

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

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

- `racadm fwupdate -s`

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

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

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

NOTA: La opción **-p** no se admite en la interfaz RACADM remota para el subcomando fwupdate.

---

getssninfo

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

En la Tabla A-11 se describe el subcomando **getssninfo**.

Tabla A-11. Subcomando getssninfo

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

Sinopsis

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

Descripción

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

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

Interfaces admitidas

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

Entrada

En la Tabla A-12 se describen las opciones del subcomando **getssninfo**.

Tabla A-12. Opciones del subcomando getssninfo

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

Ejemplos

- `racadm getssninfo`

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

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

Usuario	Dirección IP	Tipo	Consolas
root	192.168.0.10	Telnet	KVM virtual

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

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

---

getsysinfo

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

En la Tabla A-14 se describe el subcomando **racadm getsysinfo**.

Tabla A-14. getsysinfo

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

Sinopsis

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

Descripción

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

Interfaces admitidas

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

Entrada

En la Tabla A-15 se describen las opciones del subcomando **getsysinfo**.

Tabla A-15. Opciones del subcomando getsysinfo

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

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

Salida

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

Ejemplo del mensaje de salida

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
Hardware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

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

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
```

```
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

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

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

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

Ejemplos

- `racadm getsysinfo -A -s`

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

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

- `racadm getsysinfo -w -s`

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


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

Restricciones

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

---

getractime

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

En la Tabla A-16 se describe el subcomando **getractime**.

Tabla A-16. getractime

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

Sinopsis

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

Descripción

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

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

Salida

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

Ejemplo del mensaje de salida

```
racadm getractime

Jue 8 de dic 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

Interfaces admitidas

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

---

ifconfig

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

En la Tabla A-17 se describe el subcomando **ifconfig**.

Tabla A-17. ifconfig

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

Sinopsis

```
racadm ifconfig
```

---

netstat

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

En la Tabla A-18 se describe el subcomando **netstat**.

Tabla A-18. netstat

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

Sinopsis

```
racadm netstat
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

ping

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

En la Tabla A-19 se describe el subcomando **ping**.

Tabla A-19. ping

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

Sinopsis

```
racadm ping <dirección_IP>
```

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

setniccfg

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

En la Tabla A-20 se describe el subcomando **setniccfg**.

Tabla A-20. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

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

Sinopsis

```
racadm setniccfg -d

racadm setniccfg -d6

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

racadm setniccfg -s6 <dirección_IPv6> <Longitud_del_prefijo_IPv6> <puerta_de_enlace_IPv6>

racadm setniccfg -o
```

Descripción

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

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

Salida

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

Interfaces admitidas

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

---

getniccfg

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

En la Tabla A-21 se describen los subcomandos **setniccfg** y **getniccfg**.

Tabla A-21. setniccfg/getniccfg

Subcomando	Definición
getniccfg	Muestra la configuración IP actual del controlador.

Sinopsis

```
racadm getniccfg
```

Descripción

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

Ejemplo del mensaje de salida

Si la operación no es satisfactoria, el subcomando **getniccfg** muestra el mensaje de error correspondiente. De lo contrario, cuando se ejecute satisfactoriamente, el mensaje aparecerá en el formato siguiente:

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces admitidas

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

---

getsvctag

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

En la Tabla A-22 se describe el subcomando **getsvctag**.

Tabla A-22. getsvctag

Subcomando	Definición
getsvctag	Muestra la etiqueta de servicio.

Sinopsis

```
racadm getsvctag
```

Descripción

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

Ejemplo

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

```
Y76TP0G
```

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

Interfaces admitidas

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

---

racdump

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

En la Tabla A-23 se describe el subcomando **racdump**.

Tabla A-23. racdump

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

Sinopsis

```
racadm racdump
```

Descripción

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

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

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

Interfaces admitidas

- RACADM remota
- RACADM Telnet/SSH/serie

---

racreset

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

En la Tabla A-24 se describe el subcomando **racreset**.

Tabla A-24. racreset

Subcomando	Definición
racreset	Restablece el iDRAC6.

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

Sinopsis

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

Descripción

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

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

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

En la Tabla A-25 se describen las opciones del subcomando **racreset**.

Tabla A-25. Opciones del subcomando racreset

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

Ejemplos

- `racadm racreset`

  Inicia la secuencia de restablecimiento ordenado de iDRAC6.

- `racadm racreset hard`

Inicia la secuencia de restablecimiento forzado de iDRAC6.

Interfaces admitidas

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

---

racresetcfg

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

En la Tabla A-26 se describe el subcomando **racresetcfg**.

Tabla A-26. racresetcfg

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

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

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

Descripción

El comando **racresetcfg** quita todas las anotaciones de propiedad de la base de datos que hayan sido configuradas por el usuario. La base de datos tiene propiedades predeterminadas para todas las anotaciones que se usan para restablecer la tarjeta a sus valores predeterminados originales. El iDRAC6 se restablece automáticamente después de restablecer las propiedades de la base de datos.

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

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

---

serveraction

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

En la Tabla A-27 se describe el subcomando **serveraction**.

Tabla A-27. serveraction

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

Sinopsis

```
racadm serveraction <acción>
```

Descripción

El subcomando serveraction permite que los usuarios realicen operaciones de administración de la alimentación en el sistema host.En la Tabla A-28 se describen las opciones de control de alimentación de **serveraction**.

Tabla A-28. Opciones del subcomando serveraction

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

Salida

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

Interfaces admitidas

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

---

getraclog

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

En la Tabla A-29 se describe el comando **racadm getraclog**.

Tabla A-29. getraclog

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

Sinopsis

```
racadm getraclog -i

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

Descripción

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

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

- **-A**: muestra el mensaje de salida sin encabezados ni etiquetas.
- **-c**: permite introducir el número máximo de anotaciones a mostrar.
- **-m**: muestra una pantalla informativa a la vez y pregunta al usuario antes de continuar (parecido al comando **more** de UNIX).

- **-o**: muestra el mensaje de salida en una sola línea.
- **-s**: especifica la anotación inicial que se utilizará en los resultados

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

Salida

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

Ejemplo del mensaje de salida

```
Record:       1
Date/Time:    Dec 8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

Interfaces admitidas

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

---

clrraclog

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

Sinopsis

```
racadm clrraclog
```

Descripción

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

---

getsel

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

En la Tabla A-30 se describe el comando **getsel**.

Tabla A-30. getsel

Comando	Definición
getsel -i	Muestra el número de anotaciones en el Registro de sucesos del sistema.
getsel	Muestra las anotaciones del registro de sucesos del sistema.

Sinopsis

```
racadm getsel -i
```

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

Descripción

El comando **getsel -i** muestra el número de anotaciones en registro de sucesos del sistema.

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

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

-c: permite introducir el número máximo de anotaciones a mostrar.

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

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

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

-R: sólo se imprimen los datos sin procesar.

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

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

Salida

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

Por ejemplo:

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

Interfaces admitidas

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

---

clrsel

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

Sinopsis

```
racadm clrsel
```

Descripción

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

Interfaces admitidas

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

---

gettracelog

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

En la Tabla A-31 se describe el subcomando **gettracelog**.

Tabla A-31. gettracelog

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

Sinopsis

```
racadm gettracelog -i

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

Descripción

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

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

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

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

-c: especifica el número de anotaciones a mostrar

-s: especifica la anotación inicial a mostrar

-A: no muestra encabezados ni etiquetas

Salida

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

Por ejemplo:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Interfaces admitidas

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

---

sslcsrgen

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

En la Tabla A-32 se describe el subcomando **sslcsrgen**.

Tabla A-32. sslcsrgen

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

Sinopsis

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

racadm sslcsrgen -s
```

Descripción

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

Opciones

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

En la Tabla A-33 se describen las opciones del subcomando **sslcsrgen**.

Tabla A-33. Opciones del subcomando sslcsrgen

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

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

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

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

- La CSR se generó de manera satisfactoria.
- La CSR no existe.
- Generación de la CSR en progreso.

Restricciones

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

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

Ejemplos

```
racadm sslcsrgen -s
```

O bien:

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

Interfaces admitidas

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

---

sslcertupload

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

En la Tabla A-34 se describe el subcomando **sslcertupload**.

Tabla A-34. sslcertupload

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

Sinopsis

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

Opciones

En la Tabla A-35 se describen las opciones del subcomando **sslcertupload**.

Tabla A-35. Opciones del subcomando sslcertupload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertdownload

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

En la Tabla A-36 se describe el subcomando **sslcertdownload**.

Tabla A-36. sslcertdownload

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

Sinopsis

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

Opciones

En la Tabla A-37 se describen las opciones del subcomando **sslcertdownload**.

Tabla A-37. Opciones del subcomando sslcertdownload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertview

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

En la Tabla A-38 se describe el subcomando **sslcertview**.

Tabla A-38. sslcertview

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

Sinopsis

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

Opciones

En la Tabla A-39 se describen las opciones del subcomando **sslcertview**.

Tabla A-39. Opciones del subcomando sslcertview

Opción	Descripción

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

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1

Serial Number             : 00

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

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

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

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces admitidas

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

---

sslkeyupload

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

En la Tabla A-40 se describe el subcomando **sslkeyupload**.

Tabla A-40. sslkeyupload

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

Sinopsis

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

Opciones

En la Tabla A-41 se describen las opciones del subcomando **sslkeyupload**.

Tabla A-41. Opciones del subcomando sslkeyupload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

testemail

En la Tabla A-42 se describe el subcomando **testemail**.

Tabla A-42. Configuración de testemail

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

Sinopsis

```
racadm testemail -i <indice>
```

Descripción

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

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

Tabla A-43. Configuración de testemail

Acción	Comando
Activa la alerta	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Establece la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 usuario1@mi_empresa.com

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

Opciones

En la Tabla A-44 se describen las opciones del subcomando **testemail**.

Tabla A-44. Subcomandos de testemail

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

Salida

Ninguna.

Interfaces admitidas

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

---

testtrap

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

En la Tabla A-45 se describe el subcomando **testtrap**.

Tabla A-45. testtrap

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

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

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

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

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

Tabla A-46. Comandos de cfgEmailAlert

Acción	Comando
Activa la alerta	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1

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

Entrada

En la Tabla A-47 se describen las opciones del subcomando **testtrap**.

Tabla A-47. Opciones del subcomando testtrap

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

Interfaces admitidas

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

---

vmdisconnect

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

En la Tabla A-48 se describe el subcomando **vmdisconnect**.

Tabla A-48. vmdisconnect

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

Sinopsis

```
racadm vmdisconnect
```

Descripción

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

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

Interfaces admitidas

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

---

vmkey

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

En la Tabla A-49 se describe el subcomando **vmkey**.

Tabla A-49. vmkey

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

Sinopsis

```
racadm vmkey <acción>
```

Si *<acción>* se configura como reset, se restablecerá el tamaño predeterminado de 16 MB de la memoria flash virtual.

Descripción

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

Interfaces admitidas

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

---

usercertupload

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

En la Tabla A-50 se describen las opciones del subcomando **usercertupload**.

Tabla A-50. usercertupload

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

Sinopsis

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

Opciones

En la Tabla A-51 se describen las opciones del subcomando **usercertupload**.

Tabla A-51. Opciones del subcomando usercertupload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a cargar, ya sea el certificado CA o el certificado del servidor. 1 = certificado de usuario 2 = certificado de CA de usuario
-f	Especifica el nombre de archivo del certificado que se va a cargar. Si no se especifica el archivo, se seleccionará el archivo **sslcert** en el directorio actual.
-i	Número de índice del usuario. Valores válidos: de 1 a 6

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

usercertview

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

En la Tabla A-52 se describe el subcomando **usercertview**.

Tabla A-52. usercertview

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

Sinopsis

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

Opciones

En la Tabla A-53 se describen las opciones del subcomando **sslcertview**.

Tabla A-53. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado a mostrar; el certificado de usuario o el certificado de CA de usuario. 1 = certificado de usuario 2 = certificado de CA de usuario
-A	Evita la impresión de encabezados/etiquetas.
-i	Número de índice del usuario. Los valores válidos son de 1 a 6

Interfaces admitidas

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

---

localConRedirDisable

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

En la Tabla A-54 se describe el subcomando **localConRedirDisable**.

Tabla A-54. localConRedirDisable

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

Sinopsis

`racadm localConRedirDisable` *<opción>*

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

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

Interfaces admitidas

- RACADM local

Regresar a la página de contenido

Regresar a la página de contenido

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

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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

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

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

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

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

idRacProductInfo (sólo lectura)

Valores legales

Una cadena de hasta 63 caracteres ASCII.

Predeterminado

Integrated Dell Remote Access Controller

Descripción

Una cadena de texto que identifica el producto.

idRacDescriptionInfo (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres ASCII.

Predeterminado

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

Descripción

Una descripción de texto del tipo de iDRAC.

idRacVersionInfo (sólo lectura)

Valores legales

Una cadena de hasta 63 caracteres ASCII.

Predeterminado

<número de versión actual>

Descripción

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

idRacBuildInfo (sólo lectura)

Valores legales

Una cadena de hasta 16 caracteres ASCII.

Predeterminado

La versión actual de la compilación de firware del iDRAC6.

Descripción

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

idRacName (sólo lectura)

Valores legales

Una cadena de hasta 15 caracteres ASCII.

Predeterminado

iDRAC

Descripción

Un usuario asigna un nombre para identificar a este controlador.

idRacType (sólo lectura)

Valores legales

Identificación del producto

Predeterminado

10

Descripción

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

---

cfgLanNetworking

Este grupo contiene parámetros para configurar la NIC del iDRAC6

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

cfgNicIPv4Enable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la IPv4 del iDRAC6

cfgNicSelection (lectura/escritura)

Valores legales

0 = Compartido

1 = Compartido con Failover todos los controladores integrados de red

2 = Dedicaado

3= Compartido con Failover todos los controladores integrados de red (solo iDRAC6 Enterprise)

Predeterminado

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

Descripción

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

Tabla B-1. Modos admitidos de cfgNicSelection

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

cfgNicVLanEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgNicVLanId (lectura/escritura)

Valores legales

1-4094

Predeterminado

1

Descripción

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

cfgNicVLanPriority (lectura / escritura)

Valores legales

De 0 a 7

Predeterminado

0

Descripción

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

cfgDNSDomainNameFromDHCP (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgDNSDomainName (lectura / escritura)

Valores legales

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

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

Predeterminado

<vacío>

Descripción

Este es el nombre de dominio DNS.

cfgDNSRacName (lectura / escritura)

Valores legales

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

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

Predeterminado

idrac-<service tag>

Descripción

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

cfgDNSRegisterRac (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Registra el nombre del iDRAC6 en el servidor DNS.

cfgDNSServersFromDHCP (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgDNSServer1 (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IPv4 del servidor DNS 1

cfgDNSServer2 (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

Recupera la dirección IPv4 utilizada por el servidor DNS 2.

cfgNicEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgNicIpAddress (lectura/escritura)

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

Valores legales

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

Predeterminado

192.168.0.120

Descripción

Especifica la dirección IPv4 asignada al iDRAC6

cfgNicNetmask (lectura/escritura)

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

Valores legales

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

Predeterminado

255.255.255.0

Descripción

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

cfgNicGateway (lectura/escritura)

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

Valores legales

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

Predeterminado

192.168.0.1

Descripción

Dirección IPv4 de puerta de enlace del iDRAC6.

cfgNicUseDhcp (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgNicMacAddress (sólo lectura)

Valores legales

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

Predeterminado

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

Descripción

La dirección MAC de la NIC del iDRAC6.

---

cfgRemoteHosts

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

cfgRhostsFwUpdateTftpEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgRhostsFwUpdateIpAddr (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

cfgRhostsFwUpdatePath (lectura/escritura)

Valores legales

Una cadena con una longitud máxima de 255 caracteres ASCII

Predeterminado

<vacío>

Descripción

Especifica la ruta de acceso de TFTP en la que se encuentra la imagen de firmware del iRAC6 en el servidor TFTP. La ruta de acceso de TFTP es relativa a la ruta de acceso raíz de TFTP en el servidor TFTP.

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

cfgRhostsSmtpServerIpAddr (lectura/escritura)

Valores legales

Una cadena que representa una dirección IPv4válida de servidor SMTP. Por ejemplo: 192.168.0.55.

Predeterminado

0.0.0.0

Descripción

La dirección IPv4 del servidor SMTP o el servidor TFTP. El servidor SMTP transmite las alertas de correo electrónico desde el iRAC6 si las alertas están configuradas y activadas. El servidor TFTP transfiere archivos desde y hasta el iDRAC6.

---

cfgUserAdmin

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

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

cfgUserAdminIndex (sólo lectura)

Valores legales

1 - 16

Predeterminado

<instancia>

Descripción

Este número representa la instancia del usuario.

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

cfgUserAdminPrivilege (lectura/escritura)

Valores legales

0x00000000 to 0x000001ff, and 0x0

Predeterminado

0x00000000

Descripción

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

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

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

Ejemplos

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

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

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

cfgUserAdminUserName (lectura/escritura)

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

Valores legales

Una cadena de hasta 16 caracteres ASCII.

Predeterminado

root (Usuario 2)

<blank> (Todos los usuarios)

Descripción

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

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

cfgUserAdminPassword (de sólo escritura)

Valores legales

Una cadena de hasta 20 caracteres ASCII.

Predeterminado

****

Descripción

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

cfgUserAdminEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1 (Usuario 2)

0 (Todos los otros)

Descripción

Activa o desactiva un usuario individual.

cfgUserAdminSolEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el acceso de usuario Serial Over LAN (SOL) para el usuario.

cfgUserAdminIpmiSerialPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

<instancia>

Descripción

El índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la instancia de alerta.

cfgEmailAlertAddress (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgEmailAlertCustomMsg (Lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres ASCII.

Predeterminado

<vacío>

Descripción

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

---

cfgSessionManagement

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

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

cfgSsnMgtRacadmTimeout (lectura/escritura)

Valores legales

De 10 a 1920

Predeterminado

60

Descripción

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

cfgSsnMgtConsRedirMaxSessions (lectura/escritura)

Valores legales

De 1 a 4

Predeterminado

2

Descripción

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

cfgSsnMgtWebserverTimeout (lectura/escritura)

Valores legales

60 - 10800

Predeterminado

1800

Descripción

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

cfgSsnMgtSshIdleTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

300

Descripción

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

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

```
Tiempo de espera de conexión finalizado.
```

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

cfgSsnMgtTelnetTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

300

Descripción

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

Una sesión telnet finalizada muestra el siguiente mensaje de error:

```
Tiempo de espera de conexión finalizado.
```

Después de que el mensaje aparece, el sistema regresa al shell que generó la sesión Telnet.

---

cfgSerial

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

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

cfgSerialBaudRate (lectura/escritura)

Valores legales

9600, 28800, 57600, 115200

Predeterminado

57600

Descripción

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

cfgSerialConsoleEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgSerialConsoleQuitKey (lectura/escritura)

Valores legales

Una cadena de hasta 4 caracteres.

Predeterminado

^\ (<Ctrl><\>)

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

Descripción

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

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

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

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

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

cfgSerialConsoleIdleTimeout (lectura/escritura)

Valores legales

0 = Sin expiración de tiempo de espera

De 60 a 1920

Predeterminado

300

Descripción

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

cfgSerialConsoleNoAuth (lectura/escritura)

Valores legales

0 (activa la autenticación de inicio de sesión serie)

1 (desactiva la autenticación de inicio de sesión serie)

Predeterminado

0

Descripción

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

cfgSerialConsoleCommand (lectura/escritura)

Valores legales

Una cadena de hasta 128 caracteres.

Predeterminado

<vacío>

Descripción

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

cfgSerialHistorySize (lectura/escritura)

Valores legales

De 0 a 8192

Predeterminado

8 192

Descripción

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

cfgSerialCom2RedirEnable (lectura/escritura)

Predeterminado

1

Valores legales

1 (VERDADERO)

0 (FALSO)

Descripción

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

cfgSerialSshEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgSerialTelnetEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgOobSnmp

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

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

cfgOobSnmpAgentCommunity (lectura/escritura)

Valores legales

Una cadena de hasta 31 caracteres.

Predeterminado

público

Descripción

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

cfgOobSnmpAgentEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva el agente SNMP en el iDRAC6.

---

cfgRacTuning

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

cfgRacTuneConRedirPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

5900

Descripción

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

cfgRacTuneRemoteRacadmEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgRacTuneCtrlEConfigDisable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la capacidad de desactivar la facultad del usuario local para configurar el iDRAC a partir de la ROM de opción de la POST de BIOS.

cfgRacTuneHttpPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

80

Descripción

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

cfgRacTuneHttpsPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

443

Descripción

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

cfgRacTuneIpRangeEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgRacTuneIpRangeAddr (Lectura/escritura)

Valores legales

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

Predeterminado

192.168.1.1

Descripción

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

cfgRacTuneIpRangeMask (Lectura/escritura)

Valores legales

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

Predeterminado

255.255.255.0

Descripción

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

cfgRacTuneIpBlkEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgRacTuneIpBlkFailCount (Lectura/escritura)

Valores legales

De 2 a 16

Predeterminado

5

Descripción

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

cfgRacTuneIpBlkFailWindow (Lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

60

Descripción

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

cfgRacTuneIpBlkPenaltyTime (Lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

300

Descripción

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

cfgRacTuneSshPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

22

Descripción

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

cfgRacTuneTelnetPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

23

Descripción

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

cfgRacTuneConRedirEnable (Lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa redirección de la consola.

cfgRacTuneConRedirEncryptEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Cifra el vídeo en una sesión de redirección de consola.

cfgRacTuneAsrEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la función de captura de pantallas de último bloqueo del iDRAC6

cfgRacTuneLocalServerVideo (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgRacTuneLocalConfigDisable (lectura/escritura)

Valores legales

0 (VERDADERO)

1 (FALSO)

Predeterminado

0

Descripción

Desactiva el acceso al iDRAC6.

cfgRacTuneWebserverEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

<vacío>

Descripción

El nombre de host del servidor administrado.

ifcRacMnOsOsName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

<vacío>

Descripción

El nombre del sistema operativo del servidor administrado.

---

cfgRacSecurity

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

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

cfgRacSecCsrCommonName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica el Nombre Común de una CRS que debe ser un IP o el nombre del IDRAC como se expresa en el certificado.

cfgRacSecCsrOrganizationName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

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

cfgRacSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la unidad organizacional (OU) de la CSR.

cfgRacSecCsrLocalityName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la localidad (L) de la CSR.

cfgRacSecCsrStateName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

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

cfgRacSecCsrCountryCode (lectura/escritura)

Valores legales

Una cadena de hasta 2 caracteres.

Predeterminado

<vacío>

Descripción

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

cfgRacSecCsrEmailAddr (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres.

Predeterminado

<vacío>

Descripción

Especifica la dirección de correo electrónico de CSR.

cfgRacSecCsrKeySize (lectura/escritura)

Valores legales

1024

2 048

4 096

Predeterminado

1024

Descripción

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

---

cfgRacVirtual

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

cfgVirMediaAttached (lectura/escritura)

Valores legales

0 = Desconectar

1 = Conectar

2 = Auto- Conectar

Predeterminado

0

Descripción

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

cfgVirtualBootOnce (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgVirMediaFloppyEmulation (Lectura / escritura)

NOTA: Virtual Media debe volver a conectarse (utilizando cfgVirMediaAttached) para que este cambio tenga efecto.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgVirMediaKeyEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgActiveDirectory

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

cfgADRacDomain (lectura / escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

El dominio de Active Directory donde reside el iDRAC6.

cfgADRacName (lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgADDomainController1 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADDomainController2 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADDomainController3 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADAuthTimeout (lectura/escritura)

Valores legales

15 - 300 segundos.

Predeterminado

120

Descripción

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

cfgADType (lectura/escritura)

Valores legales

1 (esquema extendido)

2 (esquema estándar)

Predeterminado

1

Descripción

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

cfgADGlobalCatalog1 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADGlobalCatalog2 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADGlobalCatalog3 (Lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgADCertValidationEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

Un número entero entre 1 y 5.

Predeterminado

<instancia>

Descripción

Índice del grupo de funciones como está registrado en Active Directory

cfgSSADRoleGroupName (lectura/escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgSSADRoleGroupDomain (lectura / escritura)

Valores legales

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

Predeterminado

<vacío>

Descripción

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

cfgSSADRoleGroupPrivilege (lectura / escritura)

Valores legales

De **0x00000000** a **0x000001ff**

Predeterminado

<vacío>

Descripción

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

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

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

---

cfgIpmiSol

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

cfgIpmiSolEnable (lectura / escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva SOL.

cfgIpmiSolBaudRate (lectura/escritura)

Valores legales

9600, 19200, 57600, 115200

Predeterminado

115200

Descripción

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

cfgIpmiSolMinPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSolAccumulateInterval (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

10

Descripción

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

cfgIpmiSolSendThreshold (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

255

Descripción

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

---

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de IPMI en la LAN.

cfgIpmiLanPrivilegeLimit (Lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiLanAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgIpmiEncryptionKey (lectura/escritura)

Valores legales

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

Predeterminado

00000000000000000000

Descripción

La clave de cifrado de IPMI.

cfgIpmiPetCommunityName (lectura/escritura)

Valores legales

Una cadena de hasta 18 caracteres.

Predeterminado

público

Descripción

El nombre de comunidad SNMP para las capturas.

---

cfgIpmiPetIpv6

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

cfgIpmiPetIPv6Index (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

<Valor de índice>

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetIPv6AlertDestIpAddr

Valores legales

Dirección IPv6

Predeterminado

<vacío>

Descripción

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

cfgIpmiPetIPv6AlertEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgIpmiPef

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

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

cfgIpmiPefName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres.

Predeterminado

El nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de sucesos de plataforma.

cfgIpmiPefIndex (Lectura/escritura)

Valores legales

1 - 19

Predeterminado

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

Descripción

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

cfgIpmiPefAction (lectura/escritura)

Valores legales

0 (ninguno)

1 (apagar)

2 (restablecer)

3 (realizar ciclo de encendido)

Predeterminado

0

Descripción

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

cfgIpmiPefEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva un filtro de sucesos de plataforma específica.

---

cfgIpmiPet

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

cfgIpmiPetIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

El valor índice de una captura específica de sucesos de plataforma.

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP de destino del receptor de capturas en la red. El receptor de capturas recibe una captura SNMP cuando se presenta un suceso en el servidor administrado.

cfgIpmiPetAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva una captura específica.

---

cfgUserDomain

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

cfgUserDomainIndex (sólo lectura)

Valores legales

1 - 40

Predeterminado

Valor del índice

Descripción

Representa un dominio específico

cfgUserDomainName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres ASCII.

Predeterminado

<vacío>

Descripción

Especifica el nombre de dominio de usuario de Active Directory

---

cfgServerPower

Este grupo proporciona varias funciones de administración de alimentación.

cfgServerPowerStatus (sólo lectura)

Valores legales

1 (ENCENDIDO)

0 (del servidor, ya sea ENCENDIDO o APAGADO)

Predeterminado

<estado de alimentación del servidor actual>

Descripción

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

cfgServerPowerAllocation (sólo lectura)

NOTA: Si hay más de un suministro de energía, esta propiedad sostiene el aumento del suministro de alimentación de capacidad mínima.

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa el suministro de alimentación disponible para el uso del servidor

cfgServerActualPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa el consumo de alimentación del servidor actual

cfgServerMinPowerCapacity (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa la capacidad mínima de alimentación del servidor.

cfgServerMaxPowerCapacity (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<vacío>

Descripción

Representa la capacidad máxima de alimentación del servidor.

cfgServerPeakPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

<consumo de alimentación pico del servidor>

Descripción

Representa el consumo máximo de alimentación del servidor hasta el momento

cfgServerPeakPowerConsumptionTimestamp (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Fecha de registro del consumo máximo de alimentación

Descripción

Periodo en que se registró el consumo máximo de alimentación

cfgServerPowerConsumptionClear (sólo escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

****

Descripción

Restablece la propiedad cfgServerPeakPowerConsumption a 0 y la propiedad cfgServerPeakPowerConsumptionTimestamp a la hora actual del iDRAC

cfgServerPowerCapWatts (Lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servifor en Watts

Descripción

Representa el umbral de alimentación del servidor en Watts.

cfgServerPowerCapBtuhr (Lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servidor en BTU/hr

Descripción

Representa el umbral de alimentación del servidor expresado en BTU por hora

cfgServerPowerCapPercent (Lectura/escritura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

Umbral de alimentación del servidor en porcentaje.

Descripción

Representa el umbral de alimentación del servidor expresado en porcentajes

---

cfgIPv6LanNetworking

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

cfgIPv6Enable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la IPv6 del iDRAC6

cfgIPv6Address1 (Lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del iDRAC6

cfgIPv6Gateway (Lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 de puerta de enlace del iDRAC6.

cfgIPv6PrefixLength (Lectura/escritura)

Valores legales

1-128

Predeterminado

64

Descripción

Longitud del prefijo para dirección IPv6 del iDRAC6.

cfgIPv6AutoConfig (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la opción Auto Config de IPv6.

cfgIPv6LinkLocalAddress (sólo lectura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección local del vínculo IPv6 del iDRAC6.

cfgIPv6Address2 (sólo lectura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del iDRAC6

cfgIPv6DNSServersFromDHCP6 (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgIPv6DNSServer1 (Lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del servidor DNS

cfgIPv6DNSServer2 (Lectura/escritura)

Valores legales

Una cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Una dirección IPv6 del servidor DNS

---

cfgIPv6URL

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

cfgIPv6URLstring (sólo lectura)

Valores legales

Una cadena de hasta 80 caracteres

Predeterminado

<vacío>

Descripción

La dirección URL de la IPv6 del iDRAC6.

---

cfgIpmiSerial

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

cfgIpmiSerialConnectionMode (lectura/escritura)

Valores legales

0 (terminal)

1 (básico)

Predeterminado

1

Descripción

Cuando la propiedad **cfgSerialConsoleEnable** del DRAC 5 se establece como 0 (desactivada), el puerto serie del iDRAC6 se convierte en el puerto serie de IPMI. Esta propiedad determina el modo definido por IPMI del puerto serie.

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

cfgIpmiSerialBaudRate (lectura/escritura)

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

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

cfgIpmiSerialChanPrivLimit (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSerialFlowControl (lectura/escritura)

Valores legales

0 (ninguno)

1 (CTS/RTS)

2 (XON/XOFF)

Predeterminado

1

Descripción

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

cfgIpmiSerialHandshakeControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialLineEdit (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialEchoControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialDeleteControl (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

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

cfgIpmiSerialNewLineSequence (lectura/escritura)

Valores legales

0 (ninguno)

1 (CR-LF)

2 (NULO)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Predeterminado

1

Descripción

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

cfgIpmiSerialInputNewLineSequence (lectura/escritura)

Valores legales

0 (<ENTRAR>)

1 (NULO)

Predeterminado

1

Descripción

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

---

cfgSmartCard

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

cfgSmartCardLogonEnable (Lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

2 (Activado con RACADM remota)

Predeterminado

0

Descripción

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

cfgSmartCardCRLEnable (Lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la Lista de Revocación de Certificados (CRL)

---

cfgNetTuning

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

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

cfgNetTuningNicAutoneg (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgNetTuningNic100MB (lectura/escritura)

Valores legales

0 (10 Mb)

1 (100 Mb)

Predeterminado

1

Descripción

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

cfgNetTuningNicFullDuplex (lectura/escritura)

Valores legales

0 (Semidúplex)

1 (Dúplex completo)

Predeterminado

1

Descripción

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

cfgNetTuningNicMtu (lectura/escritura)

Valores legales

De 576 a 1500

Predeterminado

1500

Descripción

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

Regresar a la página de contenido

Regresar a la página de contenido

Interfaces admitidas de RACADM

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

La tabla a continuación contiene una descripción general de los subcomandos de RACADM y la compatibilidad correspondiente de los mismos con interfaces.

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

Subcomando	Telnet / SSH / serie	RACADM local	RACADM remota
arp	✓	✗	✓
clearascreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
usercertupload	✗	✓	✓

usercertview	✔	✔	✔
localConRedirDisable	✖	✔	✖
✔ = compatible; ✖ = no compatible			

Regresar a la página de contenido

Regresar a la página de contenido

iDRAC6 Introducción

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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

El iDRAC6 usa un microprocesador integrado de sistema en chip para el sistema de control y supervisión remoto. El iDRAC6 coexiste en la placa base con el servidor PowerEdge administrado. El sistema operativo del servidor se encarga de las aplicaciones de ejecución; 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 suceso 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 de manera predeterminada 192.168.0.120. Se debe configurar antes de que se pueda acceder al iDRAC6. Una vez que el iDRAC6 esté activado y 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 SSH y los protocolos de administración de red admitidos, por ejemplo, la Interfaz de administración de plataforma inteligente (IPMI).

Característicacs de Administración Express del iDRAC6

El iDRAC6 ofrece las siguientes funciones administrativas:

- Registro de Sistema dinámico de nombres de dominio (DDNS)
- Administración remota del sistema y supervisión utilizando una interfaz web y línea de comando SM-CLP sobre una conexión Telnet o SSH.
- Compatibilidad con la autenticación de Microsoft® Active Directory®: centraliza las identificaciones y contraseñas de usuario de iDRAC6 en Active Directory por medio del esquema estándar o de un esquema ampliado
- Supervisión: brinda acceso a la información del sistema y al estado de los componentes
- Acceso a los registros del sistema: brinda acceso al registro de sucesos del sistema, el registro del iDRAC6 y la última pantalla de bloqueo del sistema bloqueado o que no responde que es independiente del estado del sistema operativo
- Integración del software de Dell OpenManage™: permite iniciar la interfaz web del iDRAC6 desde Dell OpenManage Server Administrator o IT Assistant
- Alerta de iDRAC6: alerta sobre problemas potenciales del nodo administrado por medio de un mensaje por correo electrónico o una captura SNMP
- Administración remota de la alimentación: brinda funciones de administración remota de la alimentación, como el apagado y restablecimiento, a partir de una consola de administración
- Compatibilidad con la Interfaz de administración de plataforma inteligente (IPMI)
- Cifrado de Capa de conexión segura (SSL): ofrece administración remota y segura de sistemas por medio de la interfaz web
- Administración de seguridad a nivel de contraseña: evita el acceso no autorizado a un sistema remoto.
- Autoridad en base a funciones: proporciona permisos asignables para distintas tareas de administración de sistemas
- Soporte IPv6 - agrega soporte IPv6 como por ejemplo: proporcionar acceso a la interfaz web del iDRAC6, utilizando una dirección IPv6, especifica la dirección IPv6 para la NIC del iDRAC, especifica un número de destino para configurar un destino de alerta de IPv6 SNMP.
- Soporte de WS-MAN: ofrece administración de acceso de red mediante el uso de servicios web para protocolo de administración (WS-MAN).
- Soporte SM-CLP: agrega asistencia Administración del Servidor-Protocolo de Línea de Comandos (SM-CLP) que proporciona las regulaciones para implentaciones CLI de administración de sistemas.
- Rollback y recuperación de firmware: le permite iniciar (rollback) desde una imagen de firmware de su elección

Para mayor información acerca de iDRAC6 Express, consulte *Manual del Dueño del Hardware* en **support.dell.com\manuals.**

---

iDRAC6 Enterprise

Agrega asistencia para RACADM, KVM virtual, características de medios virtuales, una NIC dedicada, Virtual Flash (con una tarjeta de medios opcional vFlash) Para mayor información acerca de iDRAC6 Enterprise, consulte *Manual del Dueño del Hardware* en **support.dell.com\manuals.**

Características de seguridad del iDRAC6

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Autenticación de usuarios por medio de Active Directory (opcional) o identificaciones y contraseñas de usuarios almacenadas en hardware
- Autoridad en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de identificación y contraseña de usuario por medio de la interfaz web o SM-CLP
- Las interfaces SM-CLP y web interfaces, que son compatibles con los cifrados de 128 bit y 40 bit (para países en los que no se aceptan 128 bits), usando el estándar SSL 3.0
- Configuración del tiempo de espera de la sesión (en segundos) por medio de la interfaz web o SM-CLP
- Puertos IP que se pueden configurar (en los casos correspondientes)

  NOTA: Telnet no admite el cifrado SSL.

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

Plataformas admitidas

iDRAC6 admite los siguientes sistemas PowerEdge

- PowerEdge R710
- PowerEdge R610
- PowerEdge T610

Para las últimas plataformas admitidas, verifique el archivo Leeme del iDRAC6 en la *Guía de Compatibilidad Dell OpenManage Server Administrator*, en **support.dell.com\manuals** y en el DVD *Sistemas de Administración Dell Herramientas y Documentación* que fue incluido con su sistema.

Sistemas operativos admitidos

Tabla 1-1 muestra una lista de los sistemas operativos que el iDRAC6 admite.

Para la última información, consulte la *Guía de compatibilidad de Dell OpenManage Server Administrator* ubicada en el sitio de asistencia de Dell **support.dell.com\manuals** y en el DVD *Sistemas de Administración Dell Herramientas y Documentación* que fue incluido con su sistema.

Tabla 1-1. Sistemas operativos admitidos del servidor administrado

Familia de sistemas operativos	Sistema operativo
Microsoft Windows	Familia de Windows Server® 2003, incluyendo: Windows Server 2003 R2 (Web, Standard, and Enterprise Editions) con SP2 (x86) Windows Server 2003 R2 (Standard, Enterprise, and DataCenter Editions) con SP2 (x64) Windows Server 2003 (SBS, Standard, and Premium Editions) con SP2 **NOTA:** Al instalar Windows Server 2003 con Service Pack 1, tenga en cuenta los cambios de la configuración de seguridad de DCOM. Para obtener más información, consulte el artículo 903220 en el sitio web de asistencia técnica de Microsoft en **support.microsoft.com/kb/903220**. Windows Server 2008 With core (Web, Standard, and Enterprise Editions) (x86) Windows Server 2008 With core (Standard, Enterprise, and DataCenter Editions (x64) Windows Server 2008 SBS, EBS, Standard, and Premium Editions
SUSE® Linux	Enterprise Server 10 SP2
Red Hat® Linux®	Enterprise Linux 4.7 (x86_32, x86_64) Enterprise Linux 5 U2 (x86_32, x86_64)
VMware®	ESX 3.5 U4 ESXi 3.5 U4 Flash

Exploradores web admitidos

La Tabla 1-2 presenta una lista de los exploradores web que se admiten como clientes del iDRAC6.

Consulte el archivo léame del iDRAC6 y la *Guía de compatibilidad de Dell OpenManage Server Administrator* que se encuentra en el sitio web de asistencia Dell Support en **support.dell.com** para conocer información más reciente.

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

Tabla 1-2. Exploradores de web compatibles

Exploradores de web compatibles
Microsoft Internet Explorer 6.0 with SP2 for Windows XP, Windows 2000 Server, Windows 2000 Pro, Windows 2003 Server Gold, Windows 2003 Server SP1, and Windows 2003 Server SP2
Microsoft Internet Explorer 7.0 for Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows Server 2008, and Windows Vista
Mozilla Firefox 2.0 on SUSE Linux Enterprise Server (SLES) 10 SP1
Mozilla Firefox 3.0 on Windows 2003 Server Gold, Windows 2003 Server SP1, Windows 2003 Server SP2, Windows 2000 Pro, Windows XP, Windows Server 2008, Windows Vista, Red Hat Enterprise Linux 4 and 5, SLES 9 and 10, and SLES 10 SP1

Conexiones de acceso remoto admitidas

La Tabla 1-3 muestra una lista de las funciones de conexión.

Tabla 1-3. Conexiones de acceso remoto admitidas

Conexión	Características
NIC del iDRAC6	• 10Mbps/100Mbs/Ethernet • Compatibilidad con DHCP • Notificación de sucesos de correo electrónico y capturas SNMP • Compatibilidad para el shell de comandos de SM-CLP (Telnet o SSH) para operaciones como la configuración del iDRAC6, el inicio del sistema, el restablecimiento, el encendido y los comandos de apagado • Compatibilidad para las utilidades de IPMI, como IPMItool e ipmish • Conectividad en serie

Puertos del iDRAC6

La Tabla 1-4 muestra una lista de los puertos en los que el iDRAC6 detecta las conexiones. La Tabla 1-5 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 1-4. Puertos en los que el iDRAC6 detecta servidores

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

Tabla 1-5. Puertos de cliente del iDRAC6

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 útiles

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

- La ayuda en línea para el iDRAC6 proporciona información sobre el uso de la interfaz web.
- Consulte la *Guía del Usuario del Configurador del Servidor Unificado de Dell* para más información sobre la configuración de servicios de sistemas y hardware del iDRAC .
- La *Guía del usuario de Dell OpenManage IT Assistant* contiene información sobre cómo usar IT Assistant.
- Para instalar el iDRAC6, consulte *Manual del dueño del hardware* disponible en support.dell.com\manuals
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- Para las últimas plataformas admitidas, verifique el archivo Leeme del iDRAC6 en la Guía de Compatibilidad Dell OpenManage Server Administrator
- La *Guía del usuario de Dell Update Packages* contiene información acerca de cómo obtener y usar los Dell Update Packages como parte de su estrategia de actualización del sistema.
- Consulate la *Guía del Usuario de Utilidades del Controlador de Administación de Dell OpenManage Baseboard* para mayor información sobre el iDRAC6 y la interfaz IPMI

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

- En la *Guía de instalación del rack* incluida con la solución de rack se describe cómo instalar el sistema en un rack.
- En la *Guía de introducción* se ofrece una visión general sobre los componentes, la configuración y las especificaciones técnicas del sistema.
- En el *Manual del propietario del hardware* se proporciona información sobre las características del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.
- En la documentación del software de administración de sistemas se describen las funciones, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación del sistema operativo se describe cómo instalar (si es necesario), configurar y utilizar el software del sistema operativo.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- Algunas veces, con el sistema se incluyen actualizaciones que describen los cambios realizados en el sistema, en el software o en la documentación.

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

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

Regresar a la página de contenido

Regresar a la página de contenido

Configuración y uso de medios virtuales

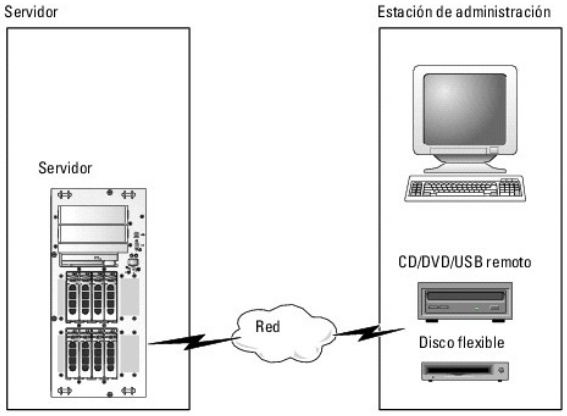
Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

---

Información general

El componente **Medios virtuales**, que puede encontrar a través del visor de redirección de consola, permite que el servidor administrado tenga acceso a medios conectados a un sistema remoto en la red.La Figura 10-1 muestra la arquitectura general de los **Medios virtuales**.

Ilustración 10-1. Arquitectura general de medios virtuales



Por medio de los **Medios virtuales**, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar archivos controladores o incluso instalar nuevos sistemas operativos de manera remota desde las unidades de CD/DVD y de disco virtuales.

NOTA: Los **medios virtuales** requieren una amplitud de banda de red mínima disponible de 128 Kbps.

Los **Medios virtuales** definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: un dispositivo de disco flexible y un dispositivo de disco óptico.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando los **Medios virtuales** se conectan, todas las solicitudes de acceso a la unidad virtual de CD o de disco flexible provenientes del servidor administrado son dirigidas a la estación de administración por la red. La conexión de los **Medios virtuales** tiene el mismo efecto que insertar discos en los dispositivos físicos. Cuando los medios virtuales no se conectan, los dispositivos virtuales no aparecen en el servidor administrado.

La Tabla 10-1 lista las conexiones compatibles de unidades ópticas virtuales y de disco flexible virtuales.

NOTA: Si cambia los **medios virtuales** mientras están conectados podría detener la secuencia de inicio de sistema.

Tabla 10-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco flexible virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 pulgadas con disquete de 1,44 pulgadas	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disco flexible USB con un disquete de 1,44 pulgadas	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44 pulgadas	Unidad USB de CD-ROM con disco CD-ROM
Disco extraíble USB	

Estación de administración con Windows

Para ejecutar el componente de **Medios virtuales** en una estación de administración que ejecuta el sistema operativo Microsoft® Windows®, instale una versión compatible de Internet Explorer o Firefox con Java Runtime Environment (JRE). Consulte "Exploradores web admitidos" para obtener detalles.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Firefox. Consulte "Exploradores web admitidos" para obtener más información.

Se requiere Java Runtime Environment (JRE) para ejecutar el complemento de redirección de consola. Puede descargar JRE desde el sitio **java.sun.com**. Se recomienda la versión 1.6 o superiores de JRE.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Seleccione **Systema→ Consola/Medios**.
3. Haga clic en **Configuración→ Medios virtuales** para configurar los valores de los medios virtuales.

   La Tabla 10-2 describe los valores de configuración de los **Medios virtuales**.
4. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 10-3.

Tabla 10-2. Propiedades de configuración de los medios virtuales

Atributo	Valor
Estado conectado de los medios remotos	**Conectar**: conecta inmediatamente los **Medios virtuales** al servidor. **Desconectar**: desconecta inmediatamente los **Medios virtuales** del servidor. **Conectar automáticamente**: conecta los **Medios virtuales** al servidor únicamente cuando se inicia una sesión de medios virtuales.
N° máx. de sesiones	Muestra el número máximo de sesiones de **medios virtuales** permitidos, que es siempre 1.
Sesiones activas	Muestra el número actual de sesiones de medios virtuales.
Cifrado activado para medios virtuales	Seleccione o deseleccione la casilla de verificación para activar o desactivar el cifrado en conexiones de **Medios virtuales**. Si está seleccionada activa el cifrado; si no está seleccionada desactiva el cifrado.
Emulación de 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** aparecerá como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB.
Activar el inicio una vez	Seleccione esta casilla para activar la opción para iniciar una vez. Esta opción automáticamente termina la sesión de **Medios virtuales** después de que el servidor se inicia una vez. Esta opción es útil para implementaciones automáticas.

Tabla 10-3. Botones de la página de configuración

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración**.
Aplicar cambios	Guarda todos los nuevos valores de configuración en la página de **configuración**.

Ejecución de los medios virtuales

PRECAUCIÓN: No emita un comando racreset cuando esté ejecutando una sesión de medios virtuales. Si lo hace, se pueden producir resultados no deseables, incluso la pérdida de datos.

NOTA: La aplicación Visor de consola debe permanecer activa mientras usted accede a los medios virtuales.

NOTA: Realice los pasos siguientes para permitir que Red Hat® Enterprise Linux® (versión 4) reconozca un dispositivo SCSI con múltiples unidades lógicas (LUN):

1. Agregue la línea siguiente a **/ect/modprobe**:

   options scsi_mod max_luns=256

cd /boot

mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp

2. Reiniciar 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 unidad de disco flexible/memoria USB/imagen/clave y una unidad óptica de su estación de administración para que esté disponible como unidad (virtual) en el servidor administrado.

Configuraciones compatibles de medios virtuales

Puede activar los medios virtuales para una unidad de 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 unidad 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 de web compatible en la estación de administración. Para obtener más información, consulte "Exploradores web admitidos".

2. Inicie la interfaz web del iDRAC6. Para obtener más información, consulte "Acceso a la interfaz web".

3. Seleccione **Systema→ Consola / Medios**.

   Aparecerá la página **Redirección de consola y medios virtuales**. Si desea cambiar los valores de cualquiera de los atributos mostrados, consulte Configuración de los medios virtuales"."

   NOTA: Es posible que aparezca **Archivo de imagen de disco flexible** bajo **Unidad de disco flexible** (si se aplica), pues este dispositivo se puede hacer un disco flexible virtual. Puede seleccionar una unidad óptica y un disco flexible al mismo tiempo para virtualizar.

   NOTA: Las letras de unidad de los dispositivos virtuales en el servidor administrado no coinciden con las letras de unidades físicas en la estación de administración.

   NOTA: Es posible que los **medios virtuales** no funcionen correctamente en los clientes con sistema operativo Windows que estén configurados con seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador del sistema.

4. Haga clic en **Iniciar el visor**.

   NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo preguntará qué desea hacer con el archivo. Elija la opción de **Abrir con el programa** y después seleccione la aplicación **javaws**, que se encuentra en el subdirectorio **bin** del directorio de instalación de JRE.

   La aplicación **Agente KVM de iDRAC** se ejecuta en otra ventana.

5. Haga clic en **Herramientas→ Ejecu**tar **Medios virtuales**.

   Aparecerá el asistente de redirección de medios.

   NOTA: No cierre este asistente a menos que desee terminar la sesión de medios virtuales.

6. Si hay algún medio conectado, deberá desconectarlo antes de conectar otro medio. Deseleccione la casilla a la izquierda del medio que desea desconectar.

7. Marque la casilla que aparece junto a los tipos de medios que desea conectar.

   Si desea conectar una imagen de disco flexible o una imagen ISO, introduzca la ruta (en el equipo local) de la imagen o haga clic en el botón **Agregar imagen...** y busque la imagen**.**

   Los medios están conectados y la ventana de **estado** se actualiza.

Desconexión de los medios virtuales

1. Haga clic en **Herramientas→ Ejecutar Medios virtuales**.

2. Deseleccione la casilla que está junto a los medios que desea desconectar.

   Los medios se desconectarán y se actualizará la ventana de **estado**.

3. Haga clic en **Salir para terminar el asistente de redirección de medios**.

Inicio desde los medios virtuales

El BIOS de sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disquete 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 el valor en el BIOS, realice los pasos a continuación:

1. Inicie el servidor administrado.
2. Presione <F2> para ingresar a la ventana de configuración del BIOS.
3. Desplácese a la secuencia de inicio y presione <Entrar>.

   En la ventana emergente, aparece una lista de las unidades virtuales ópticas y de disco flexible virtuales con otros dispositivos normales de inicio.

4. Asegúrese que la unidad virtual esté activada y que aparezca como el primer dispositivo con medio iniciable. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.
5. Guarde los cambios y salga.

   El servidor administrado se reinicia.

   El servidor administrado intenta iniciarse a partir de un dispositivo iniciable con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio iniciable está presente, el sistema se iniciará a partir del dispositivo virtual. De lo contrario, el sistema ignorará el dispositivo; como ocurriría con un dispositivo físico que no tiene medios iniciables.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas en terminar. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de los **Medios virtuales** puede tardar menos de 15 minutos en terminar. Consulte "Instalación del sistema operativo" para obtener más información.

1. Verifique lo siguiente:
   - El CD de instalación de sistema operativo está insertado en la unidad de CD de la estación de administración.
   - La unidad de CD local está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección "Inicio desde los medios virtuales" para asegurarse de que el BIOS está configurado para que inicie desde la unidad de CD a partir de la que se realiza la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

Es importante seguir estos pasos para la instalación de varios discos:

1. Desasigne el CD/DVD virtualizado (redirigido) desde la consola de medios virtuales.
2. Inserte el siguiente CD/DVD en la unidad óptica remota.
3. Asigne (redirija) este CD/DVD desde la consola de medios virtuales.

   Es posible que si inserta un nuevo CD/DVD en la unidad óptica remota sin realizar la reasignación no funcione.

Función Iniciar una vez

La función Iniciar una vez le ayuda a cambiar el orden del inicio temporalmente para iniciar desde un dispositivo remoto de medios virtuales. Esta función se usa junto con medios virtuales, generalmente, mientras se instalan sistemas operativos..

NOTA: Para usar esta función, debe tener el privilegio **Configurar el iDRAC6**.

NOTA: Los dispositivos remotos deben redirigirse mediante el uso de medios virtuales para usar esta función.

Uso de la función Iniciar una vez

1. Encienda el servidor e introduzca BIOS Boot Manager.
2. Cambie la secuencia de inicio para iniciar desde el dispositivo de medios virtuales remoto.
3. Conéctese a iDRAC6 por medio de la interfaz web y haga clic en **Sistema**→ **Consola / Medios**→ **Configuración**.
4. Marque la opción **Iniciar una vez activada** en Medios virtuales.
5. Realice un ciclo de encendido en el servidor.

   El servidor se inicia desde el dispositivo de medios virtuales remoto. La próxima vez que el servidor se reinicia, la conexión remota de medios virtuales está desconectada.

Utilización de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En sistemas con Windows, las unidades de medios virtuales se montan automáticamente cuando están conectadas y se configuran con una letra de unidad.

La utilización de las unidades virtuales desde el interior de Windows es similar a la utilización de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estarán disponibles en el sistema cuando se haga clic en la unidad y se examine el contenido de la misma.

Sistemas con Linux

En función de la configuración del software del sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, monte manualmente las unidades con el comando **mount** de Linux.

Preguntas frecuentes

La Tabla 10-4 contiene las preguntas y respuestas frecuentes.

Tabla 10-4. Uso de los medios virtuales: Preguntas frecuentes

Pregunta	Respuesta
Algunas veces noto que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?	Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Si los valores de configuración de los medios virtuales se cambian en la interfaz web del iDRAC6 o con los comandos de RACADM local, se desconectarán todos los medios conectados al momento de aplicar el cambio de configuración. Para restablecer la conexión con la unidad virtual, use el asistente de medios virtuales.
¿Qué sistemas operativos son compatibles con el iDRAC6?	Consulte "Sistemas operativos admitidos" para ver una lista de los sistemas operativos admitidos.
¿Qué exploradores web admiten el iDRAC6?	Consulte "Exploradores web admitidos" para ver una lista de los exploradores de web admitidos.
¿Por qué a veces se pierde mi conexión de cliente?	• Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD en la unidad de CD del sistema cliente, en nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión cuando el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior. • Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Asimismo, alguien puede haber cambiado los valores de configuración de los medios virtuales en la interfaz web o mediante comandos de RADACM. Para restablecer la conexión con el disco virtual, use la función de **Medios virtuales**.
La instalación del sistema operativo Windows mediante vMedia parece tardar demasiado. ¿Por qué?	Si instala el sistema operativo Windows por medio del DVD *Dell Systems Management Tools and Documentation* y la conexión de red es lenta, es posible que el procedimiento de instalación requiera más tiempo para acceder a la interfaz web del iDRAC6 debido a la latencia de la red. Mientras la ventana de instalación no indique el progreso de la instalación, significa que el procedimiento de instalación está en progreso.
¿Cómo configuro mi dispositivo virtual como dispositivo iniciable?	En el servidor administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Localice el CD virtual, el disco flexible virtual o la memoria flash virtual y cambie el orden de dispositivo de inicio según corresponda. Por ejemplo, para iniciar a partir de una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.
¿A partir de qué tipos de medios puedo iniciar el sistema?	El iDRAC6 le permite iniciar desde los siguientes medios de inicio: • Medios de CDROM/DVD de datos • Imagen ISO 9660

	• Imagen de disco flexible o disco flexible de 1,44 pulgadas • Una memoria USB a la que el sistema operativo reconoce como disco extraíble • Una imagen de memoria USB
¿Cómo puedo hacer que mi memoria USB sea iniciable?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para hacer que la memoria USB de Dell funcione como dispositivo de inicio. Usted puede iniciar también con un disco de arranque de Windows 98 y copiar los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, desde una vetana del símbolo del sistema DOS, escriba el comando siguiente: `sys a: x: /s` donde *x*: es la memoria USB que desea hacer iniciable.
No puedo encontrar mi dispositivo de 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 a mi disco flexible remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disco flexible 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 una ventana del símbolo del sistema de Linux y ejecute el siguiente comando: `grep "Disco flexible virtual" /var/log/messages` 2. Localice la última anotación de dicho mensaje y anote la hora. 3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: `grep "hh:mm:ss" /var/log/messages` donde: *hh:mm:ss* es la hora del mensaje que el comando grep informó en el paso 1. 4. En el paso 3, lea el resultado del comando grep y localice el nombre del dispositivo que se asigna al disco virtual Dell. 5. Asegúrese que está conectado a la unidad de disco flexible virtual. 6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: `mount /dev/sdx /mnt/floppy` donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
No puedo encontrar el 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 a mi 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 una ventana del símbolo del sistema de Linux y ejecute el siguiente comando: `grep "CD virtual" /var/log/messages` 2. Localice la última anotación de dicho mensaje y anote la hora. 3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: `grep "hh:mm:ss" /var/log/messages` donde hh:mm:ss es la hora del mensaje que el comando grep informó en el paso 1. 4. En el paso 3, lea el resultado del comando grep y localice el nombre de dispositivo que se asignó a "CD virtual de Dell" 5. Asegúrese de que está conectado a la unidad de CD virtual. 6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: `mount /dev/sdx /mnt/CD` donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
Cuando ejecuté una actualización de firmware de manera remota por medio de la interfaz web de iDRAC6, mis unidades virtuales en el servidor se desmontaron. ¿Por qué?	Las actualizaciones de firmware hacen que el iDRAC6 se restablezca, que abandone la conexión remota y que desmonte las unidades virtuales.
¿Por qué todos mis dispositivos USB se desconectan después de que conecto un dispositivo USB ?	Los dispositivos de medios virtuales y los dispositivos flash virtual están conectados como dispositivo USB compuesto al BUS Host USB y comparten un puerto USB común. Cuando un medio virtual o dispositivo USB flash virtual se conecta o se desconecta del BUS Host USB, todos los medios virtuales y los dispositivos flash virtual se desconectan momentáneamente del BUS Host USB y luego se conectan nuevamente.. Si el sistema operativo del host está usando un dispositivo de medios virtuales, debe evitar conectar o desconectar uno o más dispositivos de medios virtuales o flash virtual. Se recomienda que conecte todos los dispositivos USB necesarios primero, antes de usarlos.
¿Qué hace el botón restablecer USB?	Restablece los dispositivos USB remotos y locales conectados al servidor..

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de WS-Man

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

El firmware del iDRAC6 ofrece administración de acceso de red mediante el uso de servicios web para protocolo de administración (WS-MAN). WS-MAN es un mecanismo de transporte para intercambio de información. WS-MAN ofrece un idioma universal para que los dispositivos puedan compartir datos, de forma que se puedan administrar más fácilmente. WS-MAN es una parte fundamental de una solución de administración sistemas remotos, pero no es la única parte.

WS-MAN usa HTTPS para mantener el tráfico de administración seguro. El cliente debe iniciar sesión mediante el uso de privilegios de usuario local o de Microsoft® Active Directory®. HTTPS usa la Capa de conexión segura (SSL) en el puerto IP 443 para mantener comunicaciones seguras.

Los datos disponibles mediante WS-MAN son un subconjunto de datos proporcionados por la interfaz de instrumentación del iDRAC6 asignada a los siguientes perfiles de Grupo de trabajo de administración distribuida (DMTF) y perfiles de extensión de Dell.

El uso de WS-MAN para transmitir información de administración basada en CIM de DMTF es el uso más común de WS-MAN. CIM define los tipos de información de administración que pueden manipularse en un sistema administrado. Ofrece los objetos sobre los que el cliente y el servicio hablan en la conexión. WS-MAN especifica algunas acciones estándar que pueden realizarse en los objetos de administración. Por ejemplo, mediante el uso de WS-MAN, un sistema cliente puede buscar una recopilación de objetos de administración, obtener los contenidos de un objeto de administración y puede establecer sus contenidos en valores nuevos. WS-MAN ofrece los verbos de la conversación de administración; las propiedades y las clases de CIM son los sustantivos, los objetos sobre los que actúan los verbos.

Para garantizar la interoperabilidad entre los clientes y los servicios, DMTF y Dell especifican un *vocabulario* mínimo estándar de clases de CIM, propiedades y comportamientos que todas las partes deben comprender. Estos perfiles específicos de DMTF y Dell definen un conjunto de convenciones que todos los servicios que cumplen con los estándares deben implementar. Por lo tanto, todos los clientes pueden depender de estas convenciones para funcionar correctamente..

Perfiles CIM admitidos

Tabla 11-1. Perfiles CIM admitidos

DMTF estándar
1. Servidor básico Define las clases de CIM para representar el servidor host.
2. Procesador de servicio: Contiene la definición de las clases de CIM para representar el iDRAC6. **NOTA:** El Perfil básico del servidor (arriba) y el perfil de procesador de servicio son autónomos en el sentido que los objetos que describen agrupan todos los otros objetos CIM que se definen en los perfiles de componentes.
3. Propiedad física: Define las clases de CIM para representar el aspecto físico de los elementos administrados. El iDRAC6 usa este perfil para representar la información de FRU del servidor host y de sus componentes, además de la tipología física.
4. Admin de dominios SM CLP Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
5. Administración del estado de la alimentación Define las clases de CIM para las operaciones de control de alimentación. El iDRAC6 usa este perfil para las operaciones control de alimentación del servidor host.
6. Fuente de alimentación (versión 1.1) Define las clases de CIM para representar fuentes de alimentación. El iDRAC6 usa este perfil para representar las fuentes de alimentación del servidor host para describir el consumo de alimentación, como las marcas de agua de consumo de alimentación alto y bajo.
7. Servicio CLP Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
8. Interfaz IP 9. Cliente DHCP 10. Cliente DNS 11. Puerto Ethernet Los perfiles anteriores definen las clases de CIM para representar apilamientos de red. El iDRAC6 usa estos perfiles para representar la configuración 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 del RAC iDRAC6.
13. Inventario de software Define las clases de CIM para inventario de software instalado o disponible. El iDRAC6 usa este perfil para inventario de versiones de firmware del iDRAC6 actualmente instaladas mediante el protocolo TFTP.

14. Autorización basada en funciones Define las clases de CIM para representar funciones. El iDRAC6 usa este perfil para configurar privilegios de la cuenta iDRAC6.
15. Actualización de software Define las clases de CIM para inventario de actualizaciones de software disponibles. El iDRAC6 usa este perfil para inventario de actualizaciones de firmware mediante el protocolo TFTP.
16. Recopilación SMASH Define las clases de CIM para representar la configuración de CLP. El iDRAC6 usa este perfil para su propia implementación de CLP.
17. Registro de perfiles Define las clases de CIM para anunciar las implementaciones de perfil. El iDRAC6 usa este perfil para anunciar sus propios perfiles implementados, como se describe en esta tabla.
18. Medidas básicas Define las clases de CIM para representar las medidas. El iDRAC6 usa este perfil para representar las medidas del servidor host para describir el consumo de alimentación, como las marcas de agua de consumo de alimentación alto y bajo.
19. Administración de identidad simple Define las clases de CIM para representar identidades. El iDRAC6 usa este perfil para la configuración de cuentas iDRAC6.
20. Redirección de USB Define las clases de CIM para representar la redirección remota de puertos USB locales. El iDRAC6 usa este perfil junto con el perfil de medios virtuales para configurar medios virtuales.
Extensiones de Dell
1. Dell™ Active Directory Client Versión 2.0.0 Define las clases de extensiones de CIM y Dell para configurar el cliente iDRAC6 Active Directory y los privilegios locales para grupos de Active Directory.
2. Medios virtuales de Dell Define las clases de extensiones de CIM y Dell para configurar los medios virtuales de iDRAC6. Extiende el perfil de redirección de USB
3. Puerto Ethernet de Dell Define las clases de extensiones de CIM y Dell para configurar la interfaz NIC Side-Band para el NIC del iDRAC6. Extiende el perfil de puerto Ethernet.
4. Administración de la utilización de la alimentación Define las clases de extensiones de CIM y Dell para representar el presupuesto de alimentación del servidor host y para configurar/supervisar el presupuesto de alimentación del servidor host.

Para obtener más información, consulte **www.dmtf.org/standards/profiles/**. Para ver las actualizaciones para esta lista de perfiles o información, consulte las notas de publicación de WS-MAN o el archivo léame

La implementación de WS-MAN cumple con la especificación de servicios de DMTF WS-MAN versión 1.0.0. Las herramientas compatibles conocidas que admiten el protocolo WS-MAN incluyen (entre otras) las herramientas de Microsoft Windows® Remote Management (WinRM), open wsman y wsmancli.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de SM-CLP de iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección ofrece información acerca del Protocolo de línea de comandos de administración de servidor (SM-CLP) de la organización Distributed Management Task Force (DMTF) que está incorporado en el iDRAC6.

NOTA: En esta sección se parte de la premisa de que el lector está familiarizado con la iniciativa SMASH (Arquitectura de administración de sistemas para hardware de servidor) y las especificaciones de SM-CLP. Para obtener más información sobre estas especificaciones, visite el sitio web de DMTF en **www.dmtf.org**.

El SM-CLP de 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 componente de la iniciativa DMTF SMASH para simplificar la administración de servidores en varias plataformas. La especificación SM-CLP, junto con la Especificación de direccionamiento de elemento administrado y varios perfiles en las especificaciones de SM-CLP, describe los destinos y verbos estandarizados para distintas ejecuciones de trabajo de administración.

Compatibilidad con SM-CLP de iDRAC6

El SM-CLP se alberga en el firmware del controlador iDRAC6 y admite las interfaces Telnet, SSH y de conexión serie. La interfaz de SM-CLP de iDRAC6 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por la organización DMTF. SM-CLP del iDRAC6 admite todos los perfiles que se describen en Tabla 11-1 "Perfiles CIM admitidos".

Las siguientes secciones proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC6.

Funciones de SM-CLP

El SM-CLP promueve el concepto de verbos y destinos para brindar capacidades de administración de sistemas por medio de la CLI. El verbo indica la operación que se va a ejecutar y el destino determina la entidad (u objeto) que ejecuta la operación.

A continuación, se muestra un ejemplo de la sintaxis de la línea de comandos de SM-CLP.

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

Durante una sesión típica de SM-CLP, puede realizar operaciones mediante los verbos que se mencionan en la Tabla 12-1.

Tabla 12-1. Verbos CLI admitidos para el sistema

Verbo	Definición
cd	Navega en el mapa 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, verbos y destinos secundarios del destino
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 un URL a una dirección de destino especificada

Uso de SM-CLP

Establezca una conexión SSH (o Telnet) con el iDRAC6 mediante las credenciales correctas.

Se mostrará la indicación SMCLP (/admin1->).

Destinos de SM-CLP

Tabla 12-2 contiene una lista de los destinos que se proporcionan por medio de SM-CLP para sustentar las operaciones que se describen en Tabla 12-1 anteriormente.

Tabla 12-2. Destinos de SM-CLP

Destino	Definiciones
admin1	admin de dominios
admin1/profiles1	Perfiles registrados en iDRAC6
admin1/hdwr1	Hardware
admin1/system1	Destino de sistema administrado
admin1/system1/redundancyset1	Fuente de alimentación
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	Anote el destino de las recolecciones de registro.
admin1/system1/logs1/log1	Entrada de Registro de sucesos del sistema (SEL)
admin1/system1/logs1/log1/ Anotación*	Una anotación individual del registro de sucesos de sistema en el sistema administrado
admin1/system1/settings1	Configuración de recopilación del sistema administrado SMASH
admin1/system1/settings1/pwrmaxsetting1	Configuración de asignación de alimentación máxima del sistema administrado
admin1/system1/settings1/pwrminsetting1	Configuración de asignación de alimentación mínima del sistema administrado
admin1/system1/capacities1	Capacidades de recopilación del sistema administrado SMASH
admin1/system1/consoles1	Recopilación SMASH de las consolas del sistema administrado
admin1/system1/usbredirectsap1	SAP de redirección de USB de medios virtuales
admin1/system1/usbredirectsap1/remotesap1	SAP de redirección de USB de destino de medios virtuales
admin1/system1/sp1	Procesador de servicio
admin1/system1/sp1/timesvc1	Servicio de hora del procesador de servicio
admin1/system1/sp1/capabilities1	Recopilación SMASH de las capacidades del procesador de servicio
admin1/system1/sp1/capabilities1/clpcap1	capacidades del servicio CLP
admin1/system1/sp1/capabilities1/pwrmgtcap1	Capacidades del servicio de administración del estado de la alimentación en el sistema
admin1/system1/sp1/capabilities1/ipcap1	Capacidades de la interfaz IP
admin1/system1/sp1/capabilities1/dhcpcap1	Capacidades del cliente DHCP
admin1/system1/sp1/capabilities1/NetPortCfgcap1	Capacidades de configuración del puerto de red
admin1/system1/sp1/capabilities1/usbredirectcap1	SAP de redirección de USB de capacidades de medios virtuales
admin1/system1/sp1/capabilities1/vmsapcap1	Capacidades SAP de medios virtuales
admin1/system1/sp1/capabilities1/swinstallsvccap1	Capacidades de servicio de instalación de software
admin1/system1/sp1/capabilities1/acctmgtcap*	Capacidades del servicio de administración de cuenta
admin1/system1/sp1/capabilities1/adcap1	Capacidades de Active Directory
admin1/system1/sp1/capabilities1/rolemgtcap*	Capacidades de administración basada en funciones local
admin1/system1/sp1/capabilities/PwrutilmgtCap1	Capacidades administración de la 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 del (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	Configuración de recopilación de anotación del registro
admin1/system1/sp1/settings1/clpsetting1	Datos de configuración del servicio CLP
admin1/system1/sp1/settings1/ipsettings1	Datos de configuración de la asignación de la interfaz IP (estática)
admin1/system1/sp1/settings1/ipsettings1/staticipsettings1	Datos de configuración de la asignación de la interfaz IP estática
admin1/system1/sp1/settings1/ipsettings1/dnssettings1	Datos de configuración de cliente DNS
admin1/system1/sp1/settings1/ipsettings2	Datos de configuración de la asignación de la interfaz IP (DHCP)
admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1	Datos de configuración del cliente DHCP
admin1/system1/sp1/clpsvc1	Servicio de protocolo del servicio CLP
admin1/system1/sp1/clpsvc1/clpendpt*	Punto final del protocolo de servicio CLP
admin1/system1/sp1/clpsvc1/tcpendpt*	Punto final TCP del protocolo de servicio CLP
admin1/system1/sp1/jobq1	Cola de trabajo del protocolo de servicio CLP
admin1/system1/sp1/jobq1/job*	Trabajo del protocolo de 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 interfaz IP
admin1/system1/sp1/ipendpt1/gateway1	Puerta de enlace de la interfaz IP
admin1/system1/sp1/ipendpt1/dhcpendpt1	Punto final del protocolo del cliente DHCP
admin1/system1/sp1/ipendpt1/dnsendpt1	Punto final del protocolo del cliente DNS
admin1/system1/sp1/ipendpt1/dnsendpt1/dnsserver*	Servidor del cliente DNS
admin1/system1/sp1/NetPortCfgsvc1	Servicio de configuración del puerto de red
admin1/system1/sp1/lanendpt1	Punto final del LAN
admin1/system1/sp1/lanendpt1/enetport1	Puerto Ethernet
admin1/system1/sp1/VMediaSvc1	Servicio de medios virtuales
admin1/system1/sp1/VMediaSvc1/tcpendpt1	Punto final del protocolo TCP de medios virtuales
admin1/system1/sp1/swid1	Identidad de software
admin1/system1/sp1/swinstallsvc1	Servicio de instalación de software
admin1/system1/sp1/account1-16	Cuenta de autenticación multifactor (MFA)
admin1/sysetm1/sp1/account1-16/identity1	Cuenta de identidad de usuario local
admin1/sysetm1/sp1/account1-16/identity2	Cuenta de identidad de IPMI (LAN)
admin1/sysetm1/sp1/account1-16/identity3	Cuenta de identidad de IPMI (Serie)
admin1/sysetm1/sp1/account1-16/identity4	Cuenta de identidad CLP
admin1/system1/sp1/acctsvc1	Servicio de administración de cuenta de MFA
admin1/system1/sp1/acctsvc2	Servicio de administración de cuenta de IPMI
admin1/system1/sp1/acctsvc3	Servicio de administración de cuenta de CLP
admin1/system1/sp1/group1-5	Grupo de Active Directory
admin1/system1/sp1/group1-5/identity1	Identidad de Active Directory
admin1/system1/sp1/ADSvc1	Servicio de Active Directory
admin1/system1/sp1/rolesvc1	Servicio de autorización basada en funciones (RBA) local
admin1/system1/sp1/rolesvc1/Role1-16	Función local
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	Privilegio de la función local
admin1/system1/sp1/rolesvc1/Role17-21/	Función de Active Directory
admin1/system1/sp1/rolesvc1/Role17-21/privilege1	Privilegio de Active Directory
admin1/system1/sp1/rolesvc2	Servicio de RBA de IPMI
admin1/system1/sp1/rolesvc2/Role1-3	Función de IPMI
admin1/system1/sp1/rolesvc2/Role4	Función de la comunicación en serie en la LAN (SOL) de IPMI
admin1/system1/sp1/rolesvc3	Servicio CLP de RBA
admin1/system1/sp1/rolesvc3/Role1-3	Función de CLP
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	Privilegio de la función de CLP
admin1/system1/sp1/pwrutilmgtsvc1	Servicio de administración de la utilización de la alimentación
admin1/system1/sp1/pwrutilmgtsvc1/pwrcurr1	Datos de la configuración de la asignación de alimentación actual de servicio de administración de la utilización de la alimentación
admin1/system1/sp1/metricsvc1	Servicio métrico
/admin1/system1/sp1/metricsvc1/cumbmd1	Definición métrica de base acumulativa
/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	Valor métrico de base acumulativa
/admin1/system1/sp1/metricsvc1/cumwattamd1	Definición métrica de concentración acumulativa de vatios
/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	Valor métrico de concentración acumulativa de vatios
/admin1/system1/sp1/metricsvc1/cumampamd1	Definición métrica de concentración acumulativa de amp
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	Valor métrico de concentración acumulativa de amp
/admin1/system1/sp1/metricsvc1/loamd1	Definición métrica de concentración baja
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	Valor métrico de concentración baja
/admin1/system1/sp1/metricsvc1/hiamd1	Definición métrica de concentración alta
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	Valor métrico de concentración alta
/admin1/system1/sp1/metricsvc1/avgamd1	Definición métrica de concentración promedio
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	Valor métrico de concentración promedio

Regresar a la página de contenido

Regresar a la página de contenido

Instalación del sistema operativo mediante VMCLI

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

La utilidad de interfaz de línea de comandos de medios virtuales (VMCLI) es una interfaz de línea de comandos que ofrece las funciones de medios virtuales de la estación de administración al iDRAC6 en el sistema remoto. Por medio de la VMCLI y los métodos con secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad VMCLI en su red corporativa.

Antes de comenzar

Antes de usar la utilidad VMCLI, asegúrese de que los sistemas remotos de destino y la red de la empresa cumplan con los requisitos que se mencionan en las siguientes secciones.

Requisitos de los sistemas remotos

El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Una área compartida de red debe tener los componentes siguientes:

- Los archivos de sistema operativo
- Los controladores necesarios
- Los archivos de imagen de inicio del sistema operativo

El archivo de imagen debe ser un CD de sistema operativo o una imagen ISO de CD/DVD, con un formato de inicio estándar en la industria.

Creación de un archivo de imagen iniciable

Antes de instalar el archivo de imagen en los sistemas remotos, compruebe que el sistema compatible puede iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz de usuario web de iDRAC6 y luego reinicie el sistema.

Las siguientes secciones contienen información específica para la creación de archivos de imagen para los sistemas Linux y Microsoft® Windows®.

Creación de un archivo de imagen para los sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen iniciable para el sistema Linux.

Para ejecutar la utilidad, abra una ventana del 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 los sistemas Windows

Al elegir una utilidad duplicadora de datos para los archivos de imagen de Windows, seleccione una utilidad que copie el archivo de imagen y los sectores de inicio de CD/DVD.

Preparación para la instalación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que la estación de administración pueda acceder.
2. Copie los archivos de sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen iniciable preconfigurado para instalación, cree el archivo. Incluya los programas o secuencias de comandos que se vayan a utilizar para los procedimientos de instalación del sistema operativo.

   Por ejemplo, para instalar el sistema operativo Windows, el archivo de imagen puede incluir programas que sean similares a los métodos de instalación que utiliza Systems Management Server (SMS) de Microsoft.

   Al momento de crear el archivo de imagen, haga lo siguiente:

   - Siga los procedimientos estándares de instalación basada en red
   - Marque la imagen de instalación como *de sólo lectura* para garantizar que cada sistema de destino se inicie y se ejecute en el mismo procedimiento de instalación

- Realice uno de los procedimientos siguientes:
  - Integre **IPMItool** y VMCLI en la aplicación existente de instalación del sistema operativo. Use la secuencia de comandos de ejemplo **vm6deploy** como guía para usar la utilidad.
  - Utilice la secuencia de comandos **vm6deploy** existente para instalar el sistema operativo.

Instalación del sistema operativo

Use la utilidad VMCLI y la secuencia de comandos **vm6deploy** que se incluye con la utilidad para instalar el sistema operativo en los sistemas remotos.

Antes de comenzar, revise la secuencia de comandos **vm6deploy** de ejemplo que se incluye con la utilidad VMCLI. La secuencia de comandos muestra los pasos detallados que se necesitan para instalar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para instalar el sistema operativo en los sistemas remotos de destino.

1. Haga una lista de las direcciones IPv4 de iDRAC6 de los sistemas remotos que serán instalados en el archivo de texto **ip.txt**, una dirección IPv4 por línea.
2. Inserte un CD o DVD iniciable de sistema operativo en la unidad correspondiente del cliente.
3. Ejecute **vm6deploy** en la línea de comandos.

Para ejecutar la secuencia de comandos **vm6deploy**, introduzca el siguiente comando en el indicador de comandos:

```
vm6deploy -r ip.txt -u <idrac-user> -p <idrac-passwd> -c {<iso9660-img> | <path>} -f {<floppy-img>|<path>}
```

donde:

- <*usuario_del_idrac*> es el nombre de usuario del iDRAC6, por ejemplo, **root**
- <*contraseña_del_idrac*> es la contraseña del usuario del iDRAC6, por ejemplo, **calvin**
- <*imagen_iso9660*> es la ruta de acceso de la imagen ISO9660 del CD o DVD de instalación del sistema operativo
- <*ruta_de_acceso*> es la ruta de acceso del dispositivo que contiene el CD, DVD o disco flexible de instalación del sistema operativo
- <*floppy-img*> 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**. Consulte "Opciones de la línea de comandos" para obtener detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta a la opción **vmcli -r**. Si el argumento de la opción **-r** es el nombre de un archivo existente, la secuencia de comandos leerá las direcciones IPv4 de iDRAC6 del archivo especificado y ejecutará la utilidad **VMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, deberá ser la dirección de un solo iDRAC6. En este caso, la opción **-r** funciona como se describe en la utilidad **VMCLI**.

Uso de la utilidad VMCLI

La utilidad VMCLI es una interfaz de línea de comandos que admite secuencias de comandos y que suministra las funciones de medios virtuales de la estación de administración al iDRAC6.

La utilidad VMCLI presenta las siguientes características:

NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.

- Dispositivos de medios extraíbles o archivos de imagen que son congruentes con los complementos de medios virtuales
- Terminación automática cuando la opción para iniciar una vez del firmware de iDRAC6 está activada
- Comunicaciones seguras con el iDRAC6 por medio de la Capa de conexión segura (SSL)

Antes de ejecutar la utilidad, asegúrese de que cuenta con privilegios de usuario de medios virtuales en el iDRAC6.

Si el sistema operativo admite los privilegios de administrador o una pertenencia a grupos o privilegio específico del sistema operativo, también deberá tener privilegios de administrador para poder ejecutar el comando VMCLI.

El administrador del sistema cliente controla los privilegios y grupos de usuarios, por consiguiente, controla cuáles usuarios pueden ejecutar la utilidad.

Para sistemas Windows, se deben tener privilegios de usuario avanzado para poder ejecutar la utilidad VMCLI.

En los sistemas Linux, se puede acceder a la utilidad VMCLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando brinda un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos del usuario. Para agregar o editar usuarios en el grupo VMCLI, el administrador usa el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de VMCLI (o a la secuencia de comandos de VMCLI) a fin de obtener acceso al iDRAC6 en el sistema remoto y ejecutar la utilidad.

Instalación de la utilidad VMCLI

La utilidad VMCLI se encuentra en el DVD *Dell Systems Management Tools and Documentation*, que se incluye en el paquete de software Dell OpenManage System Management. Para instalar la utilidad, inserte el DVD *Dell Systems Management Tools and Documentation* en la unidad de DVD del sistema y siga las instrucciones que aparecen en la pantalla.

El DVD *Dell Systems Management Tools and Documentation* contiene los productos de software de administración de sistemas más recientes, incluso los diagnósticos, la administración de almacenamiento, el servicio de acceso remoto y la utilidad IPMItool. Este DVD también contiene archivos readme (de lectura) con la información más reciente sobre los productos de software de administración de sistemas.

Además, el DVD *Dell Systems Management Tools and Documentation* incluye **vm6deploy**: una secuencia de comandos de ejemplo que ilustra el uso de las utilidades VMCLI e IPMItool para instalar software en varios sistemas remotos.

NOTA: La secuencia de comandos **vm6deploy** depende de otros archivos que están presentes en el directorio de la misma cuando se instala. Si desea usar la secuencia de comandos desde otro directorio, deberá copiar todos los archivos con ella. Si la utilidad IPMItool no está instalada, es necesario copiarla junto con los otros archivos.

Opciones de la línea de comandos

La interfaz VMCLI es idéntica en los sistemas Windows y Linux.

El formato del comando VMCLI es el siguiente:

`VMCLI` *`[parámetro] [opciones_de_shell_de_sistema_operativo]`*

En la sintaxis de la línea de comandos se distingue entre mayúsculas y minúsculas. Consulte "Parámetros de VMCLI" para obtener más información.

Si el sistema remoto acepta los comandos y el iDRAC6 autoriza la conexión, el comando seguirá ejecutándose hasta que se presente cualquiera de los siguientes casos:

- La conexión de VMCLI termina por algún motivo.
- El proceso se termina manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, se puede usar el Administrador de tareas para terminar el proceso.

Parámetros de VMCLI

Dirección IP del iDRAC6

`-r` *`<Dirección_IP_de_iDRAC>[:<puerto_SSL_de_iDRAC>]`*

Este parámetro proporciona la dirección IPv4 del iDRAC6 y el puerto SSL, con los que la utilidad debe establecer una conexión de medios virtuales con el iDRAC6 de destino. Si introduce un nombre de DDNS o una dirección IPv4 no válida, aparecerá un mensaje de error y el comando terminará.

donde <*dirección_IP_de_iDRAC*> es una dirección IPv4 válida y única, o bien, el nombre de Sistema dinámico de nombres de dominio (DDNS) de iDRAC6 (si se admite). Si el <*Puerto_SSL_de_iDRAC*> se omite, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado de iDRAC6.

Nombre de usuario del iDRAC6

`-u` *`<nombre_de_usuario_del_iDRAC>`*

Este parámetro proporciona el nombre de usuario de iDRAC6 que ejecutará los medios virtuales.

El <*nombre_de_usuario_de_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales de iDRAC6

Si la autentificación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Contraseña de usuario del iDRAC6

`-p <contraseña_de_usuario_del_iDRAC>`

Este parámetro proporciona la contraseña para el usuario de iDRAC6 especificado.

Si la autenticación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco / disco flexible

`-f {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido (para sistemas Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

NOTA: Para la utilidad VMCLI, no se admiten puntos de montaje.

Este parámetro especifica el dispositivo o archivo que va a proporcionar el medio virtual de disco o 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 ni admitirá varios LUN. Sin embargo, el kernel admite esta funcionalidad, pero debe habilitar Red Hat Enterprise Linux versión 4 para que reconozca un dispositivo SCSI con varios LUN; para ello, siga estos pasos.

1. Edite **/etc/modprobe.conf** y agregue la siguiente línea:
   options scsi_mod max_luns=8
   (Puede especificar 8 LUN o cualquier otro número mayor que 1).

2. Obtenga el nombre de la imagen del kernel; para ello, escriba el siguiente comando en la línea de comandos:

   uname -r

3. Vaya al directorio **/de inicio** y elimine el archivo de imagen del kernel, cuyo nombre determinó en el Paso 2:

   mkinitrd /boot/initrd-'uname -r'.img `uname -r'

4. Reiniciar el servidor.

5. Ejecute el siguiente comando para confirmar que se admiten varios LUN para la cantidad de LUN que especificó en el Paso 1:

   cat /sys/modules/scsi_mod/max_luns

Si el dispositivo tiene capacidad de protección contra escritura, utilice esta capacidad para garantizar que los medios virtuales no escribirán en el medio.

Omita este parámetro de la línea de comandos si no va a virtualizar discos flexibles. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD / DVD

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o archivo que proporcionará el medio virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

`-c c:\temp\mydvd.img` (sistemas Windows)

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Microsoft® Windows®)

`-c /dev/cdrom` (sistemas Linux)

Omita este parámetro de la línea de comandos si no va a virtualizar discos CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

-v

Este parámetro se usa para mostrar la versión de la utilidad VMCLI. Si no se proporcionan otras opciones además de interruptores, el comando terminará sin mensajes de error.

Mostrar la ayuda

-h

Este parámetro muestra un resumen de los parámetros de la utilidad VMCLI. Si no se proporcionan otras opciones además de conmutadores, el comando terminará sin errores.

Datos cifrados

-e

Cuando se incluya este parámetro en la línea de comandos, VMCLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el iDRAC6 en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifrará.

NOTA: El uso de esta opción no cambia el estado de cifrado de los medios virtuales que se muestra a *habilitado* en otras interfaces de configuración del iDRAC6 como RACADM o la interfaz web.

Opciones de shell de sistema operativo de VMCLI

Las siguientes funciones del sistema operativo se pueden usar en la línea de comandos de VMCLI:

- stderr/stdout redirection: desvía los mensajes de salida impresos hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad VMCLI.

  NOTA: La utilidad VMCLI no lee la entrada estándar (**stdin**). En consecuencia, la redirección de **stdin** no es necesaria.

- Ejecución en segundo plano: de manera predeterminada, la utilidad VMCLI se ejecuta en primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en el segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter et (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

La última técnica es útil en programas de secuencias de comandos, ya que permite que la secuencia de comandos proceda después de que se inicia un nuevo proceso para el comando VMCLI (de lo contrario, la secuencia de comandos se bloqueará hasta que el programa VMCLI finalice). Cuando se inician varias instancias de VMCLI de esta manera, y una o varias de las instancias de comando se finalizan manualmente, utilice las instalaciones específicas del sistema operativo para listar y finalizar procesos.

Códigos de retorno de VMCLI

Cuando se presentan errores, se envían mensajes de texto en inglés a la salida estándar de errores.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la Interfaz de administración de plataforma inteligente (IPMI)

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

---

Configuración de IPMI

Esta sección contiene información sobre cómo configurar y usar la interfaz IPMI del iDRAC6. La interfaz incluye lo siguiente:

- IPMI mediante la LAN
- IPMI en la conexión serie
- Comunicación en serie en la LAN

El iDRAC6 es totalmente compatible con IPMI 2.0. Puede configurar la IPMI del iDRAC6 por medio de:

- la GUI del iDRAC6 de su explorador
- una utilidad de código abierto, como *IPMItool*
- el shell de IPMI de Dell™ OpenManage™, **ipmish**
- RACADM

Para obtener más información sobre cómo usar el shell de IPMI, ipmish, consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* que se encuentra disponible en **support.dell.com\manuals**.

Para obtener más información sobre cómo usar RACADM, consulte "Uso de RACADM de manera remota".

Configuración de IPMI por medio de la interfaz basada en web

Para obtener información detallada, consulte "Configuración de IPMI".

Configuración de IPMI por medio de la CLI de RACADM

1. Inicie sesión en el sistema remoto por medio de cualquiera de las interfaces de RACADM. Consulte "Uso de RACADM de manera remota".
2. Configure la IPMI en la LAN.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

   a. Actualice los privilegios de canal de IPMI.

      En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>
      ```

      donde <*nivel*> es uno de los siguientes:

      - 2 (Usuario)
      - 3 (Operador)
      - 4 (Administrador)

      Por ejemplo, para definir el privilegio de canal de LAN de IPMI en 2 (usuario), escriba el comando siguiente:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

NOTA: La IPMI del iDRAC6 es compatible con el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>`

donde <*clave*> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Actualice el nivel de privilegios mínimo de SOL de IPMI.

NOTA: El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación IPMI 2.0.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>`

donde <*nivel*> es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para configurar los privilegios de IPMI como 2 (usuario), escriba el siguiente comando:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. Actualice la velocidad en baudios de la SOL de IPMI.

NOTA: Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_en_baudios>`

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Active la SOL para un usuario individual.

NOTA: Cada usuario individual puede activar o desactivar la SOL.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <identificación> 2`

donde *<identificación>* es la identificación única del usuario.

4. Configure la conexión serie de IPMI.

a. Cambie el modo de conexión serie de IPMI al valor adecuado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

b. Establezca la velocidad en baudios de la conexión serie de IPMI.

Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

`racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <velocidad_en_baudios>`

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. Active el control de flujo del hardware de la conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

d. Establezca el nivel mínimo de privilegios de canal de conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>
```

donde *<nivel>* es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para definir los privilegios de canal de conexión serie de IPMI en 2 (usuario), escriba el siguiente comando:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. Compruebe que multiplexor serie esté configurado correctamente en el programa de configuración del BIOS.

- Reinicie el sistema.
- Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
- 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.

La configuración de IPMI ha terminado.

Si la conexión serie de IPMI está en modo de terminal, usted puede configurar los siguientes valores adicionales por medio de los comandos **racadm config cfgIpmiSerial**:

- Control de eliminación
- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Uso de la interfaz serie de acceso remoto de IPMI

Los siguientes modos están disponibles en la interfaz serie de IPMI:

- **Modo de terminal de IPMI**: admite comandos ASCII provenientes de una terminal serie. El conjunto de comandos tiene un número limitado de comandos (que incluye el control de potencia) y admite comandos de IPMI sin procesar que se introduzcan 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 la petición de comandos, escriba:

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 ó 1>
   ```

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6." para obtener información.

Configuración de la comunicación en serie en la LAN Uso de la interfaz basada en web

Para obtener información detallada, consulte "Configuración de IPMI".

NOTA: Puede usar la comunicación en serie en la LAN con las siguientes herramientas de Dell OpenManage: SOLProxy e IPMItool. Para obtener más información, consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* que se encuentra disponible en **support.dell.com\manuals**.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la utilidad de configuración del iDRAC

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

---

Información general

La utilidad de configuración de iDRAC es un entorno de configuración de preinicio que permite visualizar y establecer parámetros para iDRAC6 y para el servidor administrado. Expresamente, usted puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware de la tarjeta primaria de plano posterior
- Activar o desactivar la red de área local del iDRAC
- Activar o desactivar la IPMI sobre LAN
- Configurar los parámetros de LAN
- Configurar los medios virtuales
- Configurar Smart Card
- Cambiar el nombre de usuario administrativo y la contraseña
- Restablecer la configuración predeterminada de fábrica del iDRAC
- Ver o borrar los mensajes del registro de sucesos del sistema (SEL)
- Configurar LCD
- Configurar Sistemas de Servicios

Las tareas que puede realiazar utiliezando la utilizdad de configuración del iDRAC, también se pueden realizar con el uso de otras utilidades proporcionadas por iDRAC o el software Dell™ OpenManage™ inclusi interfaz basada en Web-, interfaz de la línea de comando SM-CLP y la interfaz de la línea de comando local RACADM.

Inicio de la utilidad de configuración del iDRAC

1. Encienda o reinicie el servidor con el botón de encendido que se encuentra en el frente del servidor.
2. Cuando aparezca el mensaje **Presione <Ctrl-E> para la configuración de acceso remoto dentro de 5 segundos.....** ,presione inmediatamente <Ctrl><E>.

NOTA: Si el sistema operativo comienza a cargarse antes de que usted presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el servidor e inténtelo otra vez.

Aparecerá la utilidad de configuración del iDRAC. Las dos primeras líneas ofrecen información sobre el firmware del iDRAC6 y las revisiones del firmware de la tarjeta primaria de plano posterior. Los niveles de revisión pueden ser útiles para determinar si una actualización de firmware es necesaria.

El firmware del iDRAC6 es la parte del firmware que se encarga de las interfaces externas, por ejemplo, la interfaz web, SM-CLP y las interfaces web. El firmware de la tarjeta primaria de plano posterior es la parte del firmware que se conecta y supervisa el entorno de hardware del servidor.

Uso de la utilidad de configuración del iDRAC

Bajo los mensajes de revisión de firmware, el resto de la utilidad de configuración del iDRAC es un menú de opciones a las que puede tener acceso por medio de las teclas de <Flecha ascendente> y <Flecha descendente>.

- Si una opción del menú conduce a un submenú o a un campo de texto editable, presione <Entrar> para acceder a la opción y <Esc> para salir de la misma después de terminar de configurarla.
- Si un elemento tiene valores que se pueden seleccionar, como Sí/No o Activado/Desactivado, presione <Flecha hacia la izquierda>, <Flecha hacia la derecha> o <Barra espaciadora> para elegir un valor.
- Si un elemento no se puede editar, aparecerá en azul. Algunos elementos se pueden editar en función de otras selecciones que usted haga.
- La línea en la parte inferior de la pantalla muestra instrucciones relacionadas con el elemento actual. Puede presionar <F1> para mostrar la ayuda del elemento actual.
- Cuando haya terminado de usar la utilidad de configuración del iDRAC, presione <Esc> para 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 iDRAC.

LAN de iDRAC6

Use la <Flecha hacia la izquierda>, la <Flecha hacia la derecha> y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**.

La LAN del iDRAC6 está desactivada en la configuración predeterminada. Es necesario activar la LAN para permitir el uso de los servicios del iDRAC6 tales como la interfaz Web, el acceso Telnet/SSH y RAC serial a la interfaz de línea de comandos de SM-CLP, la redirección de consola y los medios virtuales.

Si elige desactivar la LAN, aparecerá 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 del iDRAC, HTTP, HTTPS, Telnet o los puertos SSH, el tráfico de red de administración fuera de banda, por ejemplo, los mensajes de IPMI que se envían al iDRAC6 desde una estación de administración, no se recibe cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN de iDRAC6.

IPMI en la LAN

Presione la <Flecha hacia la izquierda>, <Flecha hacia la derecha> y la barra espaciadora para elegir entre **Activada** y **Desactivada**. Cuando se seleccione **Desactivada**, el iDRAC6 no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivada**, aparecerá la siguiente advertencia:

```
La interfaz del iDRAC IPMI fuera de banda se desactivará si el canal de LAN está desactivado.
```

Presione cualquier tecla para quitar el mensaje y continuar. Consulte LAN de iDRAC6 para ver una explicación del mensaje.

Parámetros de LAN

Presione <Entrar> para mostrar el submenú de parámetros de la LAN. Cuando haya terminado de configurar los parámetros de la LAN, presione <Esc> para volver al menú anterior.

Tabla 15-1. Parámetros de LAN

Elemento	Descripción
Valores comúnes	
Selección de NIC	Presione <Flecha Derecha>, <Flecha Izquierda >,Y barra espaceadora para cambiar entre los modos. Los modos disponibles son **Dedicado, Compartido**, **Compartido con Failover LOM2** y **Compartido con Failover All LOMs**. Estos modos le permitirán al iDRAC6 utilizar la interfaz correspondiente para la comunicación con el mundo externo.
MAC Address	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC6.
Activar VLAN	Seleccionar **Activar** para permitir el filtrado de LAN para el iDRAC6.
Identificación de VLAN	Si **VLAN Enable** es **activada**, ingrese cualquier valor VLAN ID entre 1-4094.
VLAN	Si **VLAN Enable** es **activada**, seleccione la prioridad de VLAN entre 0-7.
Registrar el nombre del iDRAC6	Seleccione **Activado** para registrar el nombre del iDRAC6 en el servicio DNS. Seleccione **Desactivado** si no desea que los usuarios puedan encontrar el nombre del iDRAC6 en el DNS.
Nombre del iDRAC6	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Entrar> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Oprima <Entrar> cuando haya terminado de modificar el nombre del iDRAC6. Oprima <Esc> para volver al menú anterior. El nombre del iDRAC6 debe ser un nombre de host DNS válido.
Nombre de dominio de DHCP	Seleccione **Activado** si desea obtener el nombre de dominio de un servicio DHCP de la red. Seleccione **Desactivado** si desea especificar el nombre de dominio.
Nombre de dominio	Si **Nombre de dominio de DHCP** esta **Desactivado**, presione <Entrar> para modificar el campo de texto **Nombre de dominio actual**. Presione <Entrar> cuando haya terminado de modificarlo. Oprima <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.
Cadena de nombre del host	Presione <Entrar> para editarla. Ingrese el nombre del host para alertas de Platform Event Trap (PET).
Alerta de LAN activada	Seleccione **Activar** para permitir un alerta de PET LAN alert.
Anotación de política de alerta 1	Seleccione **Activar** o **Desactivar** para activar el primer destino de alerta.
Destino de alerta 1	Si **LAN Alert Enabled** es **Activada**, ingrese la dirección del IP donde se emitirán las alertas de PET LAN.
Configuraciones de IPv4	Habilite o deshabilite la asisitencia para conexión IPv4.
IPv4	Seleccione soporte de protocolo IPv4 **Habilitado** o **Deshabilitado**
Clave de cifrado de RMCP+	Presione <Entrar> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado de 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.
Fuente de dirección IP	Seleccione entre **DHCP** y **Estática**. Cuando se selecciona DHCP, los campos **Dirección IP de Ethernet**, **Máscara de subred** y

	Puerta de enlace predeterminada se obtienen de un servidor DHCP. Si no se encuentra ningún servidor DHCP en la red, los campos tomarán valores de ceros. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar**.**
Dirección IP de Ethernet	Si la opción **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si la **Fuente de la 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 **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección de máscara de subred que se obtuvo de DHCP. Si la **Fuente de la 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 la **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si la **Fuente de la 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 servidor DNS. Seleccione **Desactivado** para especificar las direcciones de servidor 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.
Valores de IPv6	Habilite o Deshabilite el soporte para la conexión IPv6 .
Fuente de dirección IP	Seleccione entre **AutoConfig** y **Estática**. Cuando se selecciona **AutoConfig, los campos de dirección IPv6 1**, Longitud **del Prefijo**, y **Puerta de enlace predeterminada se obtienen a partir de** DHCP. Cuando se selecciona **Estática**, las opciones **Dirección IPv6 de Ethernet**, **Longitud del Prefijo** y **Puerta de enlace predeterminada** se pueden editar
Dirección IPv6 1	Si la opción **Fuente de la dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6
Longitud de prefijo	Configura la Longitud del Prefijo de la dirección IPv6.. Se puede valuar entre 1 y 128, inclusive.
Puerta de enlace predeterminada	Si la **Fuente de la dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada.
Dirección local IPv6	Ésta es la **dirección IPv6 local** no editable de la interfaz de la interfaz de red del iDRAC.
Dirección IPv6 2	Ésta es la **dirección IPv6 local** no editable de la interfaz de la interfaz de red del iDRAC.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidor DNS. Seleccione **Desactivado** para especificar las direcciones de servidor 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 **NIC Selection** se configura a **Dedicada**, seleccione entre **Activada** y **Desactivada** Cuando se selecciona **Activada**, la **configuración de velocidad de LAN** y la **Configuración Duplex de LAN** se configuran automáticamente.
Configuración de la velocidad de la LAN	Si se configura **Auto-Negotiate** a **Desactivado**, seleccione entre 10 Mbps y 100 Mbps.
Configuración de LAN Duplex	Si **Auto-Negotiate** se configura a **Desactivado**, seleccione entre Medio **Duplex y Duplex Total**

Configuración de medios virtuales

Medios virtuales

Presione <Enter>y seleccione **Desconectado, Conectado** o **Auto-Conectado,** Cuando se selecciona **Conectado**, los dispositivos de medios virtuales se conectan al bus USB y están listos para su uso durante las sesiones de **Redirección de consola**.

Si selecciona **Desconectado,** los usuarios no podrán acceder a los dispositivos de medios virtuales durante las sesiones de **Redirección de consola**.

NOTA: Para usar una unidad flash USB con la función de **Medios virtuales**, la opción **Tipo de emulación de unidad flash USB** debe estar establecida como **Disco duro** en la utilidad de configuración del BIOS. Se puede acceder a la utilidad de configuración del BIOS al presionar <F2> durante el arranque del servidor. Si el **Tipo de emulación de la unidad flash USB** se establece como **Automático**, la unidad flash aparecerá como unidad de disco flexible en el sistema.

Unidad flash virtual

Presione <Enter> para seleccionar **Desactivado** o **Activado.**

Activado/desactivado hace que todos los dispositivos virtuales del bus USB se **desconecten** y **conecten**.

Desactivado hace que la memoria virtual flash se elimine y deje de estar disponible para uso..

NOTA: Este campo puede ser de sólo lectura si una tarjeta SD con un tamaño superior a 256 MB no está presente en la ranura de iDRAC6 Express card.

Inicio de sesión de tarjeta inteligente

Presione <Enter> para seleccionar **Activado** or **Desactivado.**. Esta opción configura la característica Smart Card Logon. Las opciones disponibles son **Activado**, **Desactivado** y **Activado con RACADM.**

NOTA: Cuando seleccoine **Activado**, **IPMI sobre LAN** serán desactivados y bloqueados para edición.

Configuración de System Services

System Services

Presione <Enter> para seleccionar **Activado** or **Desactivado**.. Consulte la *Guía del usuario de Unified Server Configurator* disponible en el sitio Web de asistencia de Dell **support.dell.com\manuals** para obtener más información.

NOTA: Si modifica esta opción, el servidor se reiniciará cuando presione **Guarda**r y **Salir** para aplicar la nueva configuración

Cancelación de System Services

Presione <Enter> para seleccionar **No** o **Si**.

Al seleccionar **Sí,** se cierran todas las sesiones de Unified Server Configurator y el servidor se reinicia al presionar **Guardar** y **Salir** para aplicar la nueva configuración.

Configuración de LCD

Presione <Entrar> para mostrar el submenú de configuración de usuario de la **LCD**. Cuando haya terminado de configurar los parámetros de la LCD, presione <Esc> para volver al menú anterior.

Tabla 15-2. Configuración de usuario de la LCD

LCD Línea 1	Presione <Flecha Derecha>, <Flecha Izquierda >,Y barra espaceadora para cambiar entre los modos. Esta función configura el visualizador **Home** en la LCD para una de las siguientes opciones: **Ambiente Temp**, **Activar Tag**, **Nombre de Host** , **Dirección iDRAC6 IPv4** , **Dirección iDRAC6 IPv6** , **Dirección iDRAC6 MAC**, **Número de modelo**, **Ninguno**, **Servicio Tag, Alimentación del Sistema**, **cadena definida por el usuario.**
Cadena definida por el usuario para LCD	Si la **Línea 1** para LCD se configura a una **cadena definida por el Usuario,** vea o ingrese la cadena que se mostrará en la LCD La cadena puede tener un máximo de 62 caracteres.
Unidades de alimentación del sistema para LCD	Si la Línea 1 para LCD se configura a **Alimentación del Sistema,** seleccione **Watt** o **BTU/hr** para especificar la Unidad que se mostrará en la LCD.
Unidades de temperatura ambiental de LCD	Si la **Línea 1 para LCD** se configura a **Ambiente Temp**, seleccione **Celcio** o **Fahrenheit** para especificar la Unidad que se mostrará en la LCD.
Pantalla de error de LCD	Seleccione **Simple** o **SEL** (System Event Log). Esta función permite que se muestren los mensajes de errpr en la LCD en uno de los dos formatos: El formato simple provee una descripción del evento en el idioma inglés. El formato SEL muestra una cadena de textos de System Event Log.
Indicación de KVM remoto en LCD	Seleccione **Activado** para mostrar el texto*KVM* siempre que un KVM esté activado en la unidad..
Acceso al panel anterior de LCD	Presione <Flecha derecha>, <Flecha izquierda> y barra espaceadora para ver entre las opciones: **Desactivado, Ver/Modificar**, y **Solo Ver.** Esta configuración define el nivel de acceso del usuario para la LCD.

Configuración de usuario de la LAN

El usuario de la LAN es la cuenta de administrador del iDRAC, que tiene el nombre predeterminado **root**. Presione <Entrar> para mostrar el submenú de

configuración de usuario de la LAN. Cuando haya terminado de configurar el usuario de la LAN, presione <Esc> para volver al menú anterior.

Tabla 15-3. Configuración de usuario de la LAN

Elemento	Descripción
Acceso de cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione **Desactivado** para desactivar la cuenta de administrador.
Privilegio de cuenta	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Entrar> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Escriba la nueva contraseña para la cuenta de administrador. Los caracteres no aparecerán en la pantalla cuando usted los escriba.
Confirmar la contraseña	Escriba nuevamente la nueva contraseña para la cuenta de administrador. Si los caracteres que introduzca no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparecerá un mensaje y usted deberá introducir nuevamente la contraseña.

Restablecer valores predeterminados

Use la opción de menú **Restablecer valores predeterminados** para restablecer todos los valores predeterminados de fábrica de las opciones de configuración del iDRAC6 Esto puede ser necesario, por ejemplo, cuando usted ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC6 a partir de los valores predeterminados.

Presione <Entrar> para seleccionar el elemento. Aparecerá el siguiente mensaje de advertencia:

```
Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Continuar?

< NO (Cancelar) >

< SÍ (Continuar) >
```

Seleccione **SÍ** y presione <Entrar> para restablecer los valores predeterminados del iDRAC.

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 <Entrar> para mostrar el **Menú del registro de sucesos del sistema**. El sistema cuenta las anotaciones del registro y después muestra el número total de anotaciones y el mensaje más reciente. El registro de sucesos del sistema retiene un máximo de 512 mensajes.

Para ver los mensajes del registro de sucesos del sistema, seleccione **Ver registro de sucesos del sistema** y presione <Entrar>. Use la <Flecha hacia la izquierda> para retroceder al mensaje anterior (más antiguo) y <Flecha hacia la 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 de registro de sucesos del sistema.

Para borrar el registro de sucesos del sistema, seleccione **Borrar el registro de sucesos del sistema** y presione <Entrar>.

Cuando haya terminado con el menú de registro de sucesos del sistema, presione <Esc> para volver al menú anterior.

Cómo salir de la utilidad de configuración del iDRAC

Cuando haya terminado de hacer cambios en la configuración del iDRAC, presione la tecla <Esc> para mostrar el menú de salida.

Seleccione **Guardar cambios y salir** y presione <Entrar> para retener los cambios.

Seleccione **Descartar cambios y salir** y presione <Entrar> para ignorar los cambios que ha realizado

Seleccione **Regresar a la configuración** y presione <Entrar> para volver a la utilidad de configuración del iDRAC.

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alertas

Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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 Managed System, consulte la *Guía del usuario de Server Administrator*.

2. Ejecute un sistema operativo admitido Microsoft® Windows® con la función de "reinicio automático" de Windows deseleccionada en la **Configuración de inicio y recuperación de Windows**.

3. Active la pantalla de último bloqueo (desactivada de manera predeterminada).

   Para activarla por medio de RACADM local, abra una petición de comandos y escriba los comandos siguientes:

   ```
   racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
   ```

4. Active el temporizador de recuperación automática y defina la acción **Recuperación automática** como **Restablecer**, **Apagar** o **Ciclo de encendido**. Para configurar el temporizador de **Recuperación automática**, debe usar Server Administrator o IT Assistant.

   Para obtener información sobre cómo configurar el temporizador de **Recuperación automática**, consulte la *Guía del usuario de Server Administrator*. Para garantizar que se pueda capturar la pantalla de último bloqueo, el temporizador de **Recuperación automática** se debe establecer en 60 segundos o más. El valor predeterminado es de 480 segundos.

   La pantalla de último bloqueo no está disponible cuando la acción **Recuperación automática** se establece como **Apagar** o **Ciclo de encendido** si el sistema administrado está apagado.

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 iDRAC6funcione correctamente, se debe desactivar la opción **Reinicio automático** en los sistemas administrados que ejecutan los sistemas operativos Microsoft Windows® Server 2008 y Windows Server 2003.

Desactivación de la opción de reinicio automático en Windows 2008 Server

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.

2. Haga clicj en Configuración **Avanzada del Sistema** bajo **tareas** en la izquierda.

3. Haga clic en la ficha **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 **Opciones avanzadas**.

3. En **Inicio y recuperación**, haga clic en **Configuración**.

4. Deseleccione la casilla **Reiniciar automáticamente**.

5. Haga clic dos veces en **Aceptar**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma tiene un mecanismo para configurar el dispositivo de acceso remoto a fin de 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:

- Filtro de declaración crítica del ventilador
- Filtro de declaración de aviso de la bateria
- Filtro de declaración crítica de aviso de la bateria
- Filtro de declaración crítica de voltaje discreto
- Filtro de declaración de aviso de temperatura
- Filtro de declaración crítica de temperatura
- Filtro de declaración crítica de intrusión
- Filtro degradado de redundancia
- Filtro de pérdida de redundancia
- Filtro de declaración de aviso del procesador
- Filtro de declaración crítica del procesador
- Filtro ausente del procesador
- Filtro de declaración de aviso del suministro del procesador
- Filtro de declaración crítica del suministro del procesador
- Filtro de declaración ausente del suministro del procesador
- Declaración crítica de registro de sucesos
- Filtro de declaración crítica de Watchdog
- Filtro de declaración de aviso de alimentación del sistema
- Filtro de declaración crítica de aviso de alimentación del sistema

Cuando se presenta un suceso de plataforma (por ejemplo, una falla de la sonda de ventilador), el suceso se genera y se registra en el registro de sucesos del sistema. Si este suceso coincide con un filtro de sucesos de plataforma (PEF) en la lista de filtros de sucesos de plataforma de la interfaz basada en web y usted ha configurado este filtro para que genere una alerta (PET o por correo electrónico), se enviará una alerta de PET o por correo electrónico a un conjunto de uno o más destinos configurados.

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

Configuración de los 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 basada en web

Para obtener más información, consulte "Configuración de los filtros de sucesos de plataforma (PEF)".

Configuración de PEF por medio de la CLI de RACADM

1. Active el PEF.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   donde `1` y `1` son el índice de PEF y la selección de activación/desactivación, respectivamente.

   El índice de PEF puede ser un valor de 1 a 19 La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar un PEF con índice 5, escriba el comando siguiente:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. Configure las acciones de PEF.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <acción>
   ```

   donde los bits de los valores *<acción>* son los siguientes:

   - 0 = No acción de alerta.
   - 1 = apagar servidor
   - 2 = reiniciar servidor
   - 3 = apagar 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 de usuario basada en web

Para obtener más información, consulte "Configuración de capturas de suceso de plataforma (PET)".

Configuración de PET por medio de la CLI de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active la PET.

   En el indicador de comandos, escriba los comandos siguientes y pulse <Intro> después de cada uno:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1

   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   donde `1` y `1` son el índice de destino de PET y la selección de activación/desactivación, respectivamente.

   El índice de destino de PET puede ser un valor de 1 a 4. La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar una PET con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1

   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6PetAlertEnable -i 4 1
   ```

3. Configure la política de PET.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 1 <IPv4_address>

   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIPv6AlertDestIPAddr -i 1 1 <IPv6_address>
   ```

   donde `1` es el índice de destino de la PET y *<IPv4_address>* y *<IPv6_address>* son los destinos de direcciones IP 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 de usuario basada en web

Para obtener más información, consulte "Configuración de alertas por correo electrónico".

Configuración de alertas de correo electrónico por medio de la CLI de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico.

   En el indicador de comandos, escriba los comandos siguientes y pulse <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 2 (desactivado).

   Por ejemplo, para activar un correo electrónico con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configure los valores del correo electrónico.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>`

   donde `1` es el índice de destino de correo electrónico y *<dirección_de_correo_electrónico>* es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

   Para configurar un mensaje personalizado, en la petición de comandos escriba el comando siguiente y presione <Entrar>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <mensaje_personalizado>`

   donde `1` es el índice de destino de correo electrónico y *<el mensaje_personalizado>* es el mensaje que se muestra en la alerta del 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 a continuación muestra cómo probar la función de envío de alertas por correo electrónico para garantizar que el RAC pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Compruebe que los valores de **SMTP** y **Alerta por correo electrónico** estén configurados antes de probar la función de envío de alertas por correo electrónico. Consulte "Configuración de alertas por correo electrónico" para obtener más información.

Comprobación de la función de alertas de 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. Consulte las descripciones de los comandos "testtrap" y "sslkeyupload" para configurar estos valores.

Preguntas frecuentes

¿Por qué aparece el siguiente mensaje?

`Acceso remoto: error de autenticación de SNMP`

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad Get y Set del dispositivo. En IT Assistant, usted tiene el **nombre de comunidad Get = public** y el **nombre de comunidad Get = private.** De manera predeterminada, el nombre de comunidad para el agente iDRAC6 es **público**. Cuando IT Assistant envía una solicitud de comunidad Set, el agente iDRAC6 genera el error de autentificación SNMP porque sólo acepta solicitudes de **comunidad = public (público)**.

NOTA: Este nombre de comunidad de agente SNMP se utiliza para descubrimiento.

Puede cambiar el nombre de comunidad del iDRAC6 por medio de RACADM.

Para ver el nombre de comunidad del iDRAC6 , use el comando siguiente:

```
racadm getconfig -g cfgOobSnmp
```

Para ver el nombre de comunidad del iDRAC6 , use el comando siguiente:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nombre de comunidad>
```

Para acceder / configurar el nombre de comunidad de agente SNMP del iDRAC6 utilice la interfaz basada en web, diríjase a **Acceso Remoto**→ **Configuración**→ **Servicios** y haga click en agente**SNMP**

Para evitar que se generen capturas de autenticación de SNMP, se deben introducir nombres de comunidad que el agente acepte. Como el iDRAC6 sólo permite un nombre de comunidad, se debe usar el mismo nombre de comunidad **get** y **set** para la configuración de descubrimiento de IT Assistant.

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del sistema administrado

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección explica cómo realizar tareas relacionadas con la recuperación y solución de problemas de un sistema remoto bloqueado con la interfaz basada en web del iDRAC6.

- "Primeros pasos para solucionar problemas de un sistema remoto"
- "Administración de alimentación en un sistema remoto"
- "Información IPv6"
- "Cómo ver la pantalla de último bloqueo del sistema"

Primeros pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas en general en el sistema administrado:

1. ¿El sistema está encendido o apagado?
2. Si el sistema operativo está encendido, ¿se encuentra en funcionamiento, bloqueado o simplemente congelado?
3. Si está apagado, ¿se ha apagado de forma imprevista?

En el caso de sistemas bloqueados, revise la pantalla de último bloqueo (consulte "Cómo ver la pantalla de último bloqueo del sistema") y use la redirección de consolaAdministración de alimentación en un sistema remotoy la administración remota de la alimentación (consulte "") para reiniciar el sistema y observe el proceso de reinicio.

Administración de alimentación en un sistema remoto

El iDRAC6 permite realizar varias acciones de administración de la alimentación del sistema remoto, de manera que el sistema se puede recuperar después de un bloque o de algún otro suceso.

Seleccione Acciones de Control de Alimentación de la Interfaz basada en web del iDRAC6.

Para realizar acciones de de administración de energía, utilice ua Interfaz basada en web, consulte"Ejecución de operaciones de control de alimentación en un servidor."

Selección de las acciones de control de alimentación desde la CLI del iDRAC6 CLI

Use el comando `racadm serveraction` para realizar operaciones de administración de 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 encender el sistema.
- **powerstatus**: muestra el estado actual de la alimentación del servidor ("Encendido" o "Apagado")
- **hardreset**: ejecuta una operación de restablecimiento (reinicio) en el sistema administrado.

Cómo ver la información del sistema

La página **Resumen del sistema** muestra la información sobre los siguientes componentes del sistema:

- Chasis del sistema principal
- Integrated Dell Remote Access Controller 6 - Enterprise

Para acceder a la información del sistema, amplíe el árbol **Sistema** y haga clic en **Propiedades**.

Chasis del sistema principal

La Tabla 17-1 y la Tabla 17-2 describen las propiedades del chasis de sistema principal.

NOTA: Para recibir la información del **Nombre de host** y el **Nombre del sistema operativo**, deberá tener instalados los servicios de iDRAC6 en el sistema administrado.

Tabla 17-1. Campos de la información del sistema

Campo	Descripción
Descripción	Descripción del sistema.
Versión del BIOS	Versión del BIOS del sistema.
Etiqueta de servicio	Número de la etiqueta de servicio del sistema.
Nombre de host	Nombre del sistema host.
Nombre del sistema operativo	El sistema operativo que se ejecuta en el sistema.

Tabla 17-2. Campos de la recuperación automática

Campo	Descripción
Acción de recuperación	Cuando se detecta un "sistema bloqueado", se puede configurar el iDRAC6 para que ejecute una de las siguientes acciones: sin acción, restablecimiento forzado, apagar o realizar ciclo de encendido del sistema.
Cuenta regresiva inicial	El número de segundos tras la detección de un "sistema bloqueado" después de los cuales el iDRAC6 ejecutará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Integrated Dell Remote Access Controller 6 - Enterprise

Tabla 17-3Describte las propiedades de iDRAC6 Enterprise

Tabla 17-3. iD Campos de información de RAC6 Enterprise

Campo	Descripción
Fecha / Hora	Tiempo actual en la forma: Día Mes DD HH:MM:SS:YYYY
Versión del firmware	Versión del firmware del iDRAC
Firmware actualizado	La fecha del firmware fue mostrada en la forma: Día Mes DD HH:MM:SS:YYYY
Versión del hardware	Versión del Controlador de Acceso Remoto .
MAC Address	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red.

Información IPv4

Tabla 17-4 describe las propiedades IPv4

Tabla 17-4. Campos de información IPv4

Campo	Descripción
Activado	Si o No
Dirección IP	La dirección de 32-bit 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 router o un interruptor. El valor se muestra en formato de números separados con puntos, por ejemplo, 143.166.154.127.

DHCP activado	Si o No Activado indica que el protocolo de configuración dinámica de host (DHCP) está activado.

Información IPv6

Tabla 17-5 describe las propiedades IPv6

Tabla 17-5. Campos de información IPv6

Campo	Descripción
Activado	Indica si pv6 stack está activada.
IP Dirección 1	Especifica la dirección IPv6 para la interfaz de red del iDRAC NIC.
Longitud de prefijo	Un dato entero especifica la longitud del prefijo en la dirección IPv6 Se puede valuar entre 1 y 128 inclusive.
Puerta de enlace IP	Especifica la puerta de enlace para iDRAC NIC.
Dirección local de vínculo	Especifica la dirección IPv6 para la interfaz de red del iDRAC NIC.
IP Dirección 2	Especifica la dirección adicional IPv6 address para el iDRAC NIC si una está disponible.
Auto Config	AutoConfig permite que el Server Administrator obtenga la dirección IPv6 para el iDRAC NIC del servidor del Protocolo de Configuración Dinámico del Host (DHCPv6) Además, desactiva y hace salir los valores de dirección IP estática, Longitud del Prefijo y Puerta de enlace.

Uso del registro de sucesos del sistema

La página **Registro de sucesos del sistema** 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 17-6.
3. Haga clic en el botón correspondiente de la página **Registro de sucesos del sistema** para continuar (consulte la Tabla 17-6).

Tabla 17-6. Iconos de indicador de estado

Icono/categoría	Descripción
	Una marca de verificación verde indica una condición de estado sana (normal).
	Un triángulo amarillo que contiene un signo de admiración indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.
Fecha/Hora	La fecha y hora en la que se presentó el suceso. Si la fecha está en blanco, el suceso se presentó durante el inicio del sistema. El formato es mm/dd/aaaa hh:mm:ss, según el horario de 24 horas.
Descripción	Una breve descripción del suceso

Tabla 17-7. Botones de la página del registro de sucesos del sistema

Botón	Acción
Imprimir	Imprime el **registro de sucesos del sistema en el orden en que aparece en la ventana.**
Actualizar	Vuelve a cargar la página **Registro de sucesos del sistema**.
Borrar registro	Borra el **registro de sucesos del sistema**. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **registro de sucesos del sistema** en el directorio de su elección.

	NOTA: Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en support.microsoft.com.

Uso de la línea de comandos para ver el registro del sistema

```
racadm getsel -i
```

El comando **getsel -i** muestra el número de anotaciones en registro de sucesos del sistema.

```
racadm getsel <opciones>
```

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

NOTA: Consulte "getsel" para obtener más información sobre las opciones que puede usar.

El comando **clrsel** elimina todos los registros existentes del registro de sucesos del sistema.

```
racadm clrsel
```

Utilizar POST Boot Logs (Autoprueba de encendido)

NOTA: Todos los registros son eliminados despues de que se reinicia el iDRAC6..

Esta función del iDRAC6 le permite reproducir un video de imágenes detenidas de las últimas tres instancias de la prueba POST del BIOS y el inicio del sistema operativo.

Para ver los registros de captura de del inicio de POST:

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 el número de registro de captura de inicio de POST y presione **Play**.

   El video de los registros se reproducirá en una nueva pantalla.

   NOTA: Debe cerrar una captura de inicio de POST abierta antes de que genere una nueva.. No puede generar dos registros simultáneamente.
4. Haga Click en **Playback→ Play** para comenzar el video de caputra de inicio de POST..
5. Haga clic en **DETENER** para detener el video.

Cómo ver la pantalla de último bloqueo del sistema

NOTA: La función de pantalla de último bloqueo necesita que el sistema administrado tenga configurada la función **Recuperación automática** en Server Administrator. Además, asegúrese que la función **Recuperación automatizada del sistema** esté activada por medio del DRAC. Diríjase a la página **Servicios** en la ficha **Configuración** en la sección **Acceso remoto** para activar esta función.

La página **Pantalla de último bloqueo** muestra la pantalla del bloqueo más reciente, que incluye información sobre los sucesos que ocurrieron antes de que el sistema se bloqueara. La información del último bloqueo se guarda en la memoria del iDRAC6 y se puede acceder a ella de manera remota.

Para ver la página **Pantalla de último bloqueo**:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y después haga clic en **Último bloqueo pantalla**.

La página **Pantalla de último bloqueo** tiene los siguientes botones (consulte la Tabla 17-8) en la esquina superior derecha de la pantalla:

Tabla 17-8. Botones de la página Pantalla de último bloqueo

Botón	Acción
Imprimir	Imprime la página **Pantalla de último bloqueo**.
Actualizar	Vuelve a cargar la página **Pantalla de último bloqueo**.

NOTA: Debido a fluctuaciones en el temporizador de recuperación automática, es posible que la **Pantalla de último bloqueo** no se capture cuando el temporizador de restablecimiento del sistema esté definido con un valor de menos de 30 segundos. Utilice Server Administrator o IT Assistant para establecer el valor del temporizador de restablecimiento del sistema en al menos 30 segundos y garantizar que la **Pantalla de último bloqueo** funcione correctamente. Para obtener información adicional, consulte "Configuración del sistema administrado para capturar la pantalla de último bloqueo".

Regresar a la página de contenido

Regresar a la página de contenido

Recueración y solución de problemas del iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección explica cómo realizar las tareas relacionadas con la recuperación y solución de problemas de un iDRAC6 bloqueado.

Usted puede usar una de las siguientes herramientas para solucionar problemas del iDRAC6.

- Registro del RAC.
- Consola de diagnósticos
- Registro de rastreo
- racdump
- coredump

Uso del registro del RAC

El **Registro del RAC** es un registro persistente que se mantiene en el firmware del iDRAC6. El registro contiene una lista de las acciones de usuario (como inicio y cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC6.. Cuando el registro se llena, las anotaciones más antiguas se sobrescriben.

Para acceder al registro del RAC desde la interfaz de usuario del iDRAC6.

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Registros** y después haga clic en **Registro del RAC**.

El **Registro del RAC** proporciona la información que aparece en la Tabla 18-1.

Tabla 18-1. Información de la página del registro del RAC

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 de dic. 16:55:47). Cuando el iDRAC6 se inicia por primera vez y no se puede comunicar con el sistema administrado, la hora se muestra como 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.

Uso de los botones de la página de registro del RAC

La página **Registro del RAC** tiene los botones que aparecen en la Tabla 18-2.

Tabla 18-2. Botones del registro del RAC

Botón	Acción
Imprimir	Imprime la página **Registro del RAC**.
Borrar registro	Borra las anotaciones del **Registro del RAC**. **NOTA:** El botón **Borrar registro** sólo aparecerá si usted tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **Registro del RAC** en un directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en support.microsoft.com.

Actualizar	Vuelve a cargar la página **Registro del RAC**.

Utilización de la línea de comandos

Utilice el comando `getraclog` para ver las anotaciones del registro del RAC.

```
racadm getraclog -i
```

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

```
racadm getraclog [opciones]
```

NOTA: Para obtener más información, consulte "getraclog".

Puede usar el comando `clrraclog` para borrar todas las entradas del registro del RAC.

```
racadm clrraclog
```

Uso de la consola de diagnósticos

El iDRAC6 proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la Tabla 18-3) que son similares a las herramientas que se incluyen con 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.

Para acceder a la página de **Consola de diagnósticos**:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Diagnósticos**.

La Tabla 18-3 describe las opciones que están disponibles en la página **Consola de diagnóstico**. Escriba un comando y haga clic en **Enviar**. Los resultados de depuración aparecen en la página **Consola de diagnóstico**.

Para actualizar la página **Consola de diagnóstico**, haga clic en **Actualizar**. Para ejecutar otro comando, haga clic en **Volver a la página de diagnósticos**.

Tabla 18-3. 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 imprimirá información adicional acerca del tráfico en la interfaz, uso de búfer y otra información de interfaz de red.
ping *<Dirección IP>*	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo del iDRAC6. Consulte "gettracelog" para obtener más información.

Uso del registro de rastreo

El registro de rastreo del iDRAC6 es utilizado por los administradores para depurar las alertas del iDRAC6 y los problemas del sustema de red.

Para acceder al registro de rastreo desde la interfaz basada en web del iDRAC6

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
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".

El registro de rastreo recopila la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben del mismo.

- IP: rastrea los paquetes IP que se envían y reciben.

El registro de rastreo también puede contener códigos de error específicos del firmware del iDRAC6 que están relacionados con el firmware interno del iDRAC6, no con el sistema operativo del sistema administrado.

NOTA: El iDRAC6 no generará un eco para un ICMP (ping) con un tamaño de paquete mayor de 1500 bytes.

Uso de racdump

El comando **racadm racdump** proporciona un sólo comando para obtener información sobre volcado, estado e información general sobre la placa de iDRAC6

NOTA: Este comando sólo está disponible en las interfaces Telnet y SSH. Para obtener más información, consulte el comando "racdump".

Uso de coredump

El comando **racadm coredump** muestra información detallada sobre los problemas críticos recientes que se hayan presentado en el RAC. La información de volcado de núcleo se puede usar para diagnosticar estos problemas críticos.

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

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

El comando racadm coredumpdelete puede usarse para borrar los datos de **volcado de núcleo** que residan en ese momento en el RAC.

Consulte los "coredump" y "coredumpdelete" subcomandos para mayor información.

Regresar a la página de contenido

Regresar a la página de contenido

Sensores

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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 desastres tales como la inestabilidad o la caída del sistema.

Puede usar el iDRAC6 para supervisar los sensores de hardware de baterías, ventiladores, intromisión al chasis, suministros de energía, consumo de energía, temperatura y voltajes.

Sondas de baterías

Las sondas de baterías brindan información sobre el CMOS de la placa del sistema 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 ventiladores ofrecen la siguiente información:

- redundancia del ventilador: indica la capacidad del ventilador secundario de reemplazar al principal si no logra disipar el calor a una velocidad preestablecida.
- lista de sondas de ventiladores: la lista ofrece información sobre la velocidad de todos los ventiladores del sistema.

Sondas de intrusión del chasis

Las sondas de intrusión del chasis indican el estado del chasis, ya sea abierto o cerrado.

Sondas de suministros de energía

Las sondas de suministros de energía brindan la siguiente información:

- Stado del suministro de alimentación
- La redundancia del suministro de energía, esto es, la capacidad del suministro de energía redundante de reemplazar al suministro principal en caso de falla.

NOTA: Si sólo existe un suministro de energía en el sistema, la sección Redundancia de suministro de energía quedará **desactivada**.

Sondas de supervisión de la alimentación

La supervisión de la alimentación brinda información sobre el consumo de energía en *tiempo real*, en watts y amperios.

También es posible ver una representación gráfica del consumo de energía de la última hora, día o semana a partir de la fecha actual definida en el iDRAC6..

Sonda de temperatura

El sensor de temperatura brinda información sobre la temperatura ambiente de la placa del sistema. Las sondas de temperatura indican si el estado se encuentra dentro del umbral crítico y de advertencia preestablecido.

Sondas de voltaje

A continuación se enumeran las sondas de voltaje de uso habitual. Su sistema puede tener éstas y/ u otras sondas.

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

Las sondas de voltaje indican si el estado se encuentra dentro de los valores de umbral crítico y de advertencia preestablecidos.

Regresar a la página de contenido

Regresar a la página de contenido

Comenzar con iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

El iDRAC6 permite supervisar, solucionar problemas y reparar de manera remota un sistema Dell aun cuando el sistema esté apagado. El iDRAC6 ofrece un variado conjunto de funciones, por ejemplo, la redirección de consola, los medios virtuales, el KVM virtual, la autenticación de tarjeta inteligente, etc.

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

En forma opcional, puede instalar el software OpenManage™ de Dell en su management station así como también el managed system. Sin el software Managed System, usted no puede usar RACADM de manera local y el iDRAC6 no puede capturar la pantalla de último bloqueo.

Para configurar el iDRAC6 debe seguir los siguientes pasos:

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

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

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alimentación

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Los sistemas Dell™ PowerEdge™ traen muchas características nuevas y mejoradas de administración de alimentación del sistema El diseño de toda la plataforma, desde el hardware al firmware hasta el software de administración de sistema, está orientado a la eficacia energética, y a la supervisión y administración de la alimentación.

El diseño base del hardware ha sido optimizado desde una perspectiva de alimentación:

- Alta eficiencia de suministro de alimentación y reguladores de voltaje han sido incorporados en el diseño.
- Donde es posible, los componentes más bajos son seleccionados.
- El diseño de chassis ha optimizado el flujo de aire por medio del sistema para minimizar la alimentación del ventilador.

Los sistemas PowerEdge brindan muchas características para controlar y manejar la alimentación:

- **Presupuesto de alimentación: durante el inicio, un inventario del sistema permite calcular el presupuesto de alimentación de la configuración actual.**
- **Tope de alimentación**los sistemas pueden ser regulados para mantener un tope de alimentación especificado.
- **Supervisión de alimentación:** el iDRAC6 consulta a los suministros de alimentación para reunir las medidas de alimentación. El iDRAC6 junta un historial de las medidas de alimentación y calcula los promedios y picos actuales. Con la interfaz basada en web del iDRAC6 se puede ver esta información en la pantalla **Supervisión de alimentación**..

Inventario, Presupesto y Tope de Alimentación

Desde una perspectiva de utilización, usted podría tener una cantidad limitada de enfriamiento en el nivel estante. Con un tope de alimentación definido por el usuario, usted puede permitir alimentación como sea necesaria para los requisitos de su desempeño.

El iDRAC6 monitorea el consumo de alimentación y dinamicamente regula los procesadores para que cumplan con su nivel de tope definido, que maximiza el desempeño 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 basada en web o CLI de RACADM:

- Consumo acumulativo de alimentación
- Alimentación promedio, mínima y máxima
- Valores de espacio de alimentación
- Consumo de alimentación (también puede verlo en gráficas en la interfaz basada en web)

Configuración y administración de energía

Se puede usar la interfaz basada en web del iDRAC6 y la interfaz de línea de comandos (CLI) RACADM para administrar y configurar los controles de alimentación en el sistema PowerEdge. Expresamente, usted puede:

- Indica el estado de alimentación del servidor:
- Ejecutar operaciones de control de alimentación en el servidor (por ejemplo, encendido, apagado, reinicio del sistema, ciclo de alimentación).
- Ver la información del presupuesto de alimentación para el servidor y las unidades de alimentación instaladas, como consumo de alimentación potencial mínimo y máximo.
- Ver y configurar el umbral del presupuesto de alimentación del servidor.

Ver el Estado de las Unidades del Suministro de Energía

La páginas de **suministros de energía** muestra el estado y rating de las unidades del suministro de energía instaladas en el servidor.

Acceso a la interfaz basada en web

Para ver la condición de las Unidades del Suministro de Energía

1. Inicie sesión en la interfaz basada en 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:
     - **Completasl**: Suministros de energía, PS1 y PS2, son de la misma clase y funcionan apropiadamente.
     - **Perdidas**: Suministros de energía, PS1 y PS2 son diferentes clases y una de ellas no funciona correctamente. No existe redundancia.
     - **Desactivada**: Solo uno de los suministros de energía está disponible. No existe redundancia.
   - **Elementos de suministro de energía individuales:** los posibles valores son:
     - **Estado**muestra lo siguiente:
       - **OK** Indica que la unidad de suministro de energía está presente y comunica con el servidor.
       - **Aviso** indica que sólo se han emitido alertas de advertencia y que se debe realizar una acción correctiva dentro del marco de tiempo establecido por el administrador. Si no se realizan acciones correctivas dentro del tiempo especificado por el administrador, se podrían producir fallas críticas o graves que pueden afectar la integridad del servidor.
       - **Severo** indica que se ha emitido al menos una alerta de falla. El estado de falla indica una falla de alimentación en el servidor y se debe realizar una acción correctiva inmediatamente.
     - **Ubicación** muestra el nombre de la unidad de suministro de energía: PS-n donde n es el número de suministro de energía.
     - **Tipo** muestra el tipo de suministro de energía, como AC o DC (AC-a-DC o DC-a-DC conversión de voltaje).
     - **Potencia de entrada** muestra la potencia de entrada de suministro de energía que es una carga máxima de energía AC que el sistema podría colocar en el centro de datos.
     - **Potencia máxima** muestra la potencia máxima de suministro de energía, donde el suministro de energía DC está 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 ok, entrada perdida, ausente o falla predictiva.
     - **Versión FW** muestra la versión firmware version del suministro de energía

NOTA: La máxima potencia es diferente que la potencia de entrada debido a la eficiencia de suministro de energía. Por ejemplo, si la eficiencia del suministro de energía es 89% y la Potencia Máxima es 717W, la Potencia de Entrada se estima a 797W.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

Ver el presupuesto de alimentación

El CMC proporciona descripciones generales del estado de la alimentación del subsistema de energía en la página **Estado del presupuesto de alimentación**.

Por medio de la interfaz web

NOTA: Para realizar acciones de administración de alimentación, se debe contar con privilegios de **Administrador**.

1. Inicie sesión en la interfaz basada en web del iDRAC6 .
2. Haga clic en la ficha **Power Management** (Administración de energía).
3. Selecione la opción **Presupuesto de alimentación** .
4. Se muestra la página **Power Budget Status (Estado de consumo máximo)**.

La primera tabla muestra los límites mínimos y máximos de los umbrales de alimentación especificados por el usuario para la configuración del sistema actual. Estos representan el rango de consumos de energía AC que usted podría configurar como límite del sistema. Una vez selecciono, este límite podría ser la carga de alimentación AC máxima que el sistema pudiera colocar en el centro de datos.

Consumo de energía potencial mínimo muestra el valor más bajo del Umbral de Presupuesto de Alimentación que usted podría especificar..

Consumo de energía potencial máximo muestra el valor más alto del Umbral de Presupuesto de Alimentación que usted podría especificar. Este valor es también el consumo de alimentación máximo absoluto de la configuración actual del sistema.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el iDRAC, inicie sesión y escriba:

```
racadm getconfig -g cfgServerPower
```

NOTA: Para obtener más información acerca de cfgServerPower, incluso los detalles de mensajes de salida, consulte "cfgServerPower

---

Umbral de Presupuesto de Alimentación

El Umbral de Presupuesto de Alimentación, si está activado, permite establecer un límite de energía para el sistema. El rendimiento del sistema se ajusta en forma dinámica a fin de mantener el consumo de 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 chequean **Activado** para Umbral de Presupuesto de Alimentación, el sistema implementará el umbral especificado por el usuario. Si **no chequea** el valor del Umbral de Presupuesto de Alimentación, el sistema no tendrá límite de alimentación. Por ejemplo, para una determinada configuración del sistema, el consumo de energía potencial máximo es 700 W y el consumo de energía mínimo potencial 500 W. Puede especificar y activar un Umbral de Presupuesto de Alimentación para reducir el consumo desde 650W and 500W. Desde ese punto en el desempeño del sistema, se ajustará dinámicamente para mantener el consumo de energía de modo que no exceda el umbral especificado del usuario de 525W.

Acceso a la interfaz basada en web

1. Inicie sesión en la interfaz basada en web del iDRAC6 .
2. Haga clic en la ficha **Power Management** (Administración de energía).
3. Selecione la opción **Presupuesto de alimentación** . Se muestra la página **Power Budget Status (Estado de consumo máximo**).
4. Ingrese un valor en **Watts, BTU/hr** o porcentaje en la tabla de Umbral de Presupuesto de alimentación. El valor que especifique en Watts o BTU/hr será el valor límite del umbral del presupuesto de alimentación. Si especifica un valor de porcentaje, será un porcenataje de intervalo Consumo de Energía Potencial Máximo-a-Mínimo.. Por ejemplo, el Consumo de Energía Potencial Máximo de 100% y a su vez 0% significa Consumo de Energía Potencial Mínimo.

   NOTA: El Umbral de Presupuesto de Alimentación no puede ser mayor al Consumo de Energía Potencial Máximo o menor al Consumo de Energía Potencial Mínimo.

5. Verifique **Activado** para activar el umbral o dejelo sin verificar. Si especifica **Activado**, el sistema implementará el umbral especificado del usuario. Si no lo **verifica**, el sistema no tendrá límite de alimentación
6. Haga clic en **Aplicar cambios**.

Uso de RACADM

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <valor máximo de alimentación expresado en vatios>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <valor máximo de alimentación expresado en vatios>

racadm config -g cfgServerPower -o - cfgServerPowerCapPercent <valor máximo de alimentación expresado en porcentajes>
```

NOTA: Cuando configuere el umbral del presupuesto de alimentación en BTU/hr, la conversión a Watts se redondea al más cercano. Cuando se vuelve a leer el umbral del presupuesto de alimentación, la conversión de Watts a BTU/hr vuelve a redondearse. Como resultado, el valor escrito pordría ser nominalmente diferente al valor leído, por ejemplo, un umbral establecido a 600 BTU/hr será leído como 601 BTU/hr.

Ver la supervisión de alimentación

Por medio de la interfaz web

ra ver la información de supervisión de alimentación:

1. Inicie sesión en la interfaz basada en web del iDRAC6 .
2. Seleccione **Suministros de energía** en el árbol del sistema. Se muestra la página **Power Control** (Control de alimentación).

La información brindad en la página de **Supervisión de alimentación** se describe a continuación.

Supervisión de alimentación

- **Estado**: **OK** indica que las unidades de de suministro de energía están presentes y se comunican con el servidor, **Aviso** indica que una alerta de aviso ha sido emitida y **Severo** indica que una alerta de falla ha sido emitida.
- **Nombre de la sonda**: nivel del sistema de la placa del sistema. La descripción indica que la sonda está supervisada por su ubicación en el sistema.
- **Lectura: el consumo de energía actual en vatios**.

Amperaje

- **Ubicación** muestra el nombre de la unidad de suministro de energía: PS-n donde n es el número de suministro de energía.
- **Lectura**: The current power consumption in amperios.

Estadísticas de seguimiento de alimentación

NOTA: Hay un defecto por resolver en la lista del tiempo y maximo de tiempo. El valor mostrado debajo del tiempo de corriente es en realidad el tiempo máximo y el valor debajo del tiempo máximo es el tiempo de corriente

- **Acumulado** Indica el consumo acumulado actual de energía de todos los módulos en el chasis medido desde la entrada de los suministros de energía. Los valores son visualizados en KWh y el valor acumulado que es el total de energía utilizada por el sistema. Puede restablecer el valor con la tecla **Restablecer acumulado**.
- **Max Peak Amps** especifica el valor de corriente maximo dentro el intervalo especificado por el Inicio y los tiempos de corriente. Puede restablecer el valor con la tecla **Restablecer picos máximos**.
- **Max Peak Amps** especifica el valor de corriente maximo dentro el intervalo especificado por el Inicio y los tiempos de corriente. Puede restablecer el valor con la tecla **Restablecer picos máximos**.
- **Start Time** muestra la fecha y la hora registrados cuando se borró por última vez el valor de consumo de energía del sistema, y comenzó el nuevo ciclo de mediciones. Para **Acumulativo**, puede reestablecer este cvalor con la tecla **Reset Cumulative**, pero podrá persistir por medio de una operación de failover o restablecimiento del sistema. Para **Max Peak Amps** y **Max Peak Watts**, puede restablecer este valor con la tecla **Reset Max Peaks** ,pero podrá persistir por medio de na operación de failover o restablecimiento del sistema.
- **La Hora actual de medición** para la **Alimentación acumulada del sistema** muestra la fecha y hora en las que se calculó el consumo de energía del sistema para su visualización. Para **Max Peak Amps** y **Max Peak Watts**, los campos de **Hora actual de medición** muestran el tiempo cuando estos picos ocurren.

NOTA: Las Estadísticas de seguimiento de alimentación se mantienen en caso de restablecimientos del sistema y reflejan toda la actividad en el intervalo entre las horas de Inicio y Finalización establecidas. El botón **Restablecer picos máximos** restablecerá los valores estadísticos de picos. En la tabla siguiente, la información de Consumo de alimentación no se mantiene en caso de restablecimiento del sistema por lo que se restablecerá a los valores pico estadísticos. Los valores de alimentación que se muestran son promedios acumulados en el intervalo de tiempo respectivo (minuto, hora, día y semana previos). Debido a que los intervalos de tiempo de inicio y fin pueden ser distintos de aquellos de las estadísticas de seguimiento de alimentación, los valores de alimentación pico (picos máximos en vatios en comparación con consumo máximo de alimentación) pueden ser distintos.

Consumo de alimentación

- Muestra el promedio, consumo de alimentación máximo y mínimo en el sistema para el último minuto, hora, día y semana.
- Consumo de alimentación promedio: promedio sobre minuto, hora, día y mes anteriores. .
- Consumo de alimentación máximo y Consumo de alimentación mínimo: el consumo de alimentación máximo y mínimo observado dentro de un intervalo de tiempo determinado
- Tiempo máximo y mínimo: el tiempo en el que se producen consumos de alimentación máximos y mínimos.

Headroom

El Headroom instantáneo del sistema muestra la diferencia entre la alimentación disponible en las unidades de suministro de energía y el consumo de alimentación actual del sistema.

El Headroom máximo del sistema muestra la diferencia entre la alimentación disponible en las unidades de suministro de energía y el consumo de alimentación máximo del sistema.

Mostrar gráfica

Al hacer click en esta tecla, se muestra la gráfica de la Alimentación del iDRAC6 y el Consumo de Corriente en Watts y Amperios, respectivamente en la última hora. El usuario tiene la opción de ver estas estadísticas hasta una semana antes, con el menú que se desliza hascia abajo provisto arriba de las gráficas.

NOTA: Cada uno de los puntos de información de la gráfica representa el promedio de lecturas en un lapso de 5 minutos. Como resultado, es posible que la gráfica no refleje fluctuaciones breves de alimentación ni tampoco el consumo actual.

Ejecución de operaciones de control de alimentación en un servidor

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

El iDRAC6 le permite efectuar en forma remota varias acciones de administración de energía, como un apagado ordenado.

Por medio de la interfaz web

1. Inicie sesión en la interfaz basada en web del iDRAC6 .
2. Haga clic en la ficha **Power Management** (Administración de energía). Se muestra la página **Power Control** (Control de alimentación).
3. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
   - **Encender el sistema**: enciende el sistema (equivalente a pulsar el botón de encendido cuando el servidor está Apagado). Esta acción se desactivará si el servidor ya está Encendido.
   - **Apagar el sistema** apaga la alimentación del sistema. Esta acción se desactivará si el servidor ya está Apagado.
   - **NMI (Interrupción no enmascarable) genera una NMI para detener el sistema.**
   - **Apagado normal** apaga el sistema..
   - **Restablecer el sistema (reinicio mediante sistema operativo):** reinicia el sistema sin apagarlo. Esta acción se desactivará si el sistema ya está Apagado.
   - **Ciclo de encendido del sistema (inicio en frío)** apaga el sistema y luego lo reinicia. Esta acción se desactivará si el sistema ya está Apagado.
4. Haga clic en **Aplicar**. Aparece un cuadro de diálogo que le solicita confirmación.
5. Haga clic en **OK** (Aceptar) para realizar la acción de administración de energía (por ejemplo, hacer que se reinicie el sistema).

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el servidor, inicie sesión y escriba::

```
racadm serveraction <acción>

donde <acción> es encendido, apagado, ciclo de encendido, apagado no ordenado, o estado de alimentación.
```

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de las funciones de seguridad

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

El iDRAC6 proporciona las siguientes funciones de seguridad:

- Opciones de seguridad avanzada para el administrador del iDRAC6:
  - La opción de desactivación de la redirección de consola permite que el usuario *local* del sistema desactive la redirección de consola por medio de la función de redirección de consola del iDRAC6.
  - Las funciones de desactivación de la configuración local permiten que el administrador del iDRAC6 *remoto* desactive de manera selectiva la capacidad de configurar el iDRAC6 a partir de:
    - La ROM de opción de la POST del BIOS
    - El sistema operativo por medio de racadm local y las utilidades de Dell OpenManage™ Server Administrator
- La operación de la interfaz basada en web y la CLI 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 sesión (en segundos) mediante la interfaz basada en web o la CLI de RACADM
- Puertos IP que se pueden configurar (en los casos correspondientes)
- Secure Shell (SSH), que utiliza una capa cifrada de transporte para brindar una mayor seguridad.
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.
- Rango limitado de direcciones IP para clientes que se conectan al iDRAC6

Opciones de seguridad avanzada para el administrador del iDRAC6:

Desactivar la configuración local del iDRAC6

Los administradores pueden desactivar la configuración local por medio de la interfaz gráfica de usuario del iDRAC6 al seleccionar **Acceso remoto**→ **Configuración**→ **Servicios**. Cuando se selecciona la casilla **Desactivar la configuración local del iDRAC por medio de la ROM de opción**, la utilidad de configuración del iDRAC6 -a la cual 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 mediante Dell OpenManage Server Administrator, pero aún pueden leer los valores de la configuración.

Los administradores pueden activar una de estas opciones al mismo tiempo o ambas. Además de activarlas por medio de la interfaz gráfica de usuario, los administradores también pueden utilizar los comandos locales de RACADM.

Desactivación de la configuración local durante el reinicio del sistema

Esta función desactiva la capacidad que tiene el usuario del sistema administrado de configurar el iDRAC6 durante el reinicio del sistema.

```
racadm config -g cfgRacTuning -o

cfgRacTuneCtrlEConfigDisable 1
```

NOTA: Esta opción es respaldada solo en la utilidad de configuración del iDRAC6. Para actualizarse con esta versión, actualice el BIOS por medio del paquete de actualización del BIOS que se encuentra s**itio web de**e asistencia técnica de Dell en support.dell.com.

Desactivación de la configuración local a partir de RACADM local

Esta función desactiva la capacidad del usuario del sistema administrado de configurar el iDRAC6 por medio de las utilidades de RACADM local o de Dell OpenManage Server Administrator.

```
racadm config -g cfgRacTuning -o cfgRacTuneConRedirEncryptEnable 1
```

PRECAUCIÓN: Estas funciones limitan en gran medida la capacidad del usuario local para configurar el iDRAC6 desde el sistema local, lo que incluye el restablecimiento de la configuración predeterminada. Dell recomienda que se utilicen estas funciones a discreción y se debe desactivar sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión.

NOTA: Para obtener más información, consulte del 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 de asistencia técnica de Dell en **support.dell.com**.

Aunque los administradores pueden establecer las opciones de configuración local por medio de los comandos de racadm local, por motivos de seguridad sólo pueden restablecerlos a partir de una interfaz de línea de comandos o una interfaz basada en web del iDRAC6 fuera de banda. La opción `cfgRacTuneLocalConfigDisable` se aplica después de que la autoprueba de encendido del sistema ha terminado y el sistema ha terminado de iniciar el entorno de sistema operativo. El sistema operativo puede ser un sistema tal como Microsoft® Windows Server® o Enterprise Linux que pueda ejecutar localmente comandos de racadm, o bien un sistema operativo de uso limitado tal como el Entorno de Preinstalación de Microsoft Windows® o vmlinux, utilizado para ejecutar los comandos de racadm locales de Dell OpenManage Deployment Toolkit

Hay varias situaciones que pueden requerir que los administradores desactiven la configuración local. Por ejemplo, en un centro de datos con varios administradores para servidores y dispositivos de acceso remoto, es posible que los responsables de mantener las pilas de software de servidor no necesiten tener acceso a los dispositivos de acceso remoto. Asimismo, los técnicos pueden tener acceso físico a los servidores durante mantenimiento de rutina de sistemas -durante el cual pueden reiniciar los sistemas y acceder al BIOS protegido con contraseña- pero no deben tener la facultad de configurar los dispositivos de acceso remoto. En situaciones de este tipo, es recomendable que los administradores de dispositivos de acceso remoto desactiven la configuración local.

Los administradores deben tener presente que debido a que la desactivación de la configuración local limita en gran medida los privilegios de configuración local -incluso la capacidad de restablecer la configuración predeterminada del iDRAC6- sólo deben utilizar estas opciones cuando sea necesario y normalmente deberán desactivar sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión. Por ejemplo, si los administradores han deshabilitado a todos los usuarios locales del iDRAC6 y sólo permiten que los usuarios del servicio de directorio Microsoft Active Directory® inicien sesión en el iDRAC6, y posteriormente falla la infraestructura de autenticación de Active Directory, es posible que los administradores no puedan iniciar sesión. Asimismo, si los administradores han desactivado toda la configuración local e incorporan un iDRAC6 con una dirección IP estática a una red que ya incluye un servidor de Protocolo de configuración de host dinámica (DHCP), y éste luego asigna la dirección IP del iDRAC6 a otro dispositivo de la red, debido al conflicto resultante existe la posibilidad de que se desactive la conectividad fuera de banda del DRAC, lo que obliga a los administradores a restablecer la configuración predeterminada del firmware por medio de una conexión serie.

Desactivar el Remote Virtual KVM del iDRAC6

Los administradores pueden desactivar de manera selectiva el KVM virtual del iDRAC6, lo que brinda un mecanismo seguro y flexible para que el usuario local trabaje en el sistema sin que alguien más vea las acciones del usuario a través de la redirección de consola. El uso de esta función requiere la instalación de software de nodo administrado del iDRAC en el servidor. Los administradores pueden desactivar el vKVM remoto con el siguiente comando:

```
racadm LocalConRedirDisable 1
```

El comando LocalConRedirDisable desactiva las ventanas de sesión vKVM remota existentes cuando se ejecuta con el argumento 1

Para ayudar a evitar que el usuario remoto anule la configuración del usuario local, este comando sólo está disponible para racadm local. Los administradores pueden usar este comando en los sistemas operativos que admiten racadm local, incluso en Microsoft Windows Server 2003 y SUSE Linux Enterprise Server 10. Como los efectos de este comando continúan después de reinicios del sistema, los administradores deben revertirlo específicamente para reactivar el vKVM remoto. Pueden hacer esto con el argumento 0:

```
racadm LocalConRedirDisable 0
```

Hay varias situaciones que pueden requerir la desactivación del vKVM remoto del iDRAC6. Por ejemplo, es posible que los administradores no deseen que un usuario del iDRAC6 remoto vea la configuración del BIOS que han establecido en un sistema, en tal caso, pueden desactivar el vKVM remoto durante la POST del sistema por medio del comando `LocalConRedirDisable`. Si también desean aumentar la seguridad a través de la desactivación automática del vKVM remoto cada vez que un administrador inicie sesión en el sistema, lo pueden hacer mediante la ejecución del comando `LocalConRedirDisable` en las secuencias de comandos de inicio de sesión del usuario.

NOTA: Para obtener más información, consulte del 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 de asistencia técnica de Dell en **support.dell.com**.

Para obtener más información sobre las secuencias de comando de inicio de sesión, consulte **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx.**

Cómo asegurar las comunicaciones de 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 conexión segura (SSL)"
- "Solicitud de firma de certificado (CSR)"
- "Acceso al menú principal de SSL"
- "Generación de una solicitud de firma de certificado"

Capa de conexión segura (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 la Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas y es una técnica ampliamente aceptada para ofrecer comunicación cifrada y autenticada entre los clientes y servidores a fin de evitar intercepción furtiva a la información de la red.

Un sistema habilitado para SSL:

- Se autentica a sí mismo en un cliente habilitado para SSL
- Permite que el cliente se autentique a sí mismo en el servidor
- Permite que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado brinda una protección de datos de alto nivel. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está generalmente disponible para los exploradores de Internet en Norteamérica.

El servidor web del iDRAC6 incluye un certificado digital SSL firmado automáticamente de Dell (identificación de servidor). Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del servidor web mediante el envío de una solicitud al iDRAC6 para generar una nueva solicitud de firma de certificado (CSR).

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (CA) para obtener un certificado de servidor seguro. Los certificados de servidor seguro protegen la identidad de un sistema remoto y garantizan que otros usuarios no puedan ver o cambiar la información que se intercambia con dicho sistema. Para garantizar la seguridad del DRAC, se recomienda enfáticamente que se genere una CSR, se envíe a una autoridad de certificados y se cargue el certificado devuelto por la autoridad de certificados.

Una autoridad emisora de certificados es una entidad comercial que está reconocida por la industria de la tecnología informática por cumplir estándares altos de revisión confiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Después de recibir la solicitud CSR, la autoridad de certificados (CA) revisa y verifica la información que contiene. Si el candidato cumple los estándares de seguridad de la autoridad de certificados, ésta emite un certificado al candidato que lo identifica de forma exclusiva para transacciones a través de redes y en Internet.

Después de que la CA aprueba la CSR y le envía un certificado, se debe cargar el certificado en el firmware del iDRAC6 La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **SSL**.

Utilice el **Menú Principal de SSL** (veaTabla 21-1) para generar una CSR, cargar un certificado de servidor existente o ver un certificado de servidor existente. La información de la CSR se almacena en el firmware del iDRAC6..La Tabla 21-2 describe los botones disponibles en la página **Menú principal de SSL**.

Tabla 21-1. Menú principal SSL

Campo	Descripción
Solicitud de firma de certificado (CSR)	Haga clic en **Siguiente** para abrir la página Generación de una solicitud de firma de certificado, que permite generar una CSR para su envío a una CA para solicitar un certificado web seguro.
Cargar certificado de servidor	Haga clic en **Siguiente** para cargar un certificado existente sobre el que su compañía tenga derechos y que utiliza para controlar el acceso al iDRAC6. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509, base 64. No se aceptan los certificados codificados con DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su iDRAC6
Ver el certificado de servidor	Haga clic en **Siguiente** para ver un certificado de servidor existente.

Tabla 21-2. Botones del menú principal de SSL

Botón	Descripción
Imprimir	Imprime la página **Menú principal de** SSL.
Actualizar	Vuelve a cargar la página **Menú principa**l de SSL.
Next	Avanza a la página siguiente.

Generación de una solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribe la CSR anterior en el firmware. Antes de que iDRAC pueda acetar su CR firmado, la CSR en el firmware debe coincidir con el certificado que CA devuelve.

1. En la página **Menú principal d**e SSL, seleccione **Generar una nueva 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 21-3 describe las opciones de la página **Generar solicitud de firma de certificado (CSR)**.

3. Haga click en **Generar** para abrir o guardar la CSR

4. Haga clic en el botón de la página **Generar solicitud de firma de certificado (CSR)** para continuar.La Tabla 21-4 describe los botones que están disponibles en la página **Generar solicitud de firma de certificado (CSR)**.

Tabla 21-3. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **www.empresaxyz.com**). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Grupo de empresa). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Monterrey). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo o algún otro carácter.
Nombre del estado:	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Nuevo León). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación. Utilice el menú desplegable para seleccionar el país.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Puede escribir la dirección de correo electrónico de su empresa o cualquier dirección de correo electrónico que desee tener asociada con la CSR. Este campo es opcional.

Tabla 21-4. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime la página **Generar solicitud de firma de certificado (CSR)**.
Actualizar	Imprime la página **Generar solicitud de firma de certificado (CSR)**.
Volver al menú principal de SSL	Regresa a la página **Menú principal de SSL**.
Generar	Genera una CSR.

Cómo ver un certificado de servidor

1. En la página **Menú principal de SSL**, seleccione **Ver certificado de servidor** y haga clic en **Siguiente**.

   La Tabla 21-5 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Haga clic en el botón correspondiente de la página **Ver certificado de servidor** para continuar.

Tabla 21-5. Información de certificados

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

Uso de Secure Shell (SSH)

Para obtener más información sobre SSH, consulteUso de Secure Shell (SSH)

Configuración de servicios

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**. Además, la utilidad de línea de comandos de RACADM sólo se puede activar si el usuario ha iniciado sesión como **root**.

1. Amplíe el árbol de **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Servicios**.
3. Configure los servicios siguientes según sea necesario:
   - Configuración local (Tabla 21-6)
   - Servidor web (Tabla 21-7)
   - SSH (Tabla 21-8)
   - Telnet (Tabla 21-9)
   - RACADM remota (Tabla 21-10)
   - Agente SNMP (Tabla 21-11)
   - Agente de recuperación automatizada del sistema (Tabla 21-12)

   Utilice el **Agente de recuperación automatizada del sistema** para activar la función de **Pantalla de último bloqueo** del iDRAC6.

   NOTA: Server Administrator debe estar instalado con la función **Recuperación automática** activada mediante el establecimiento de **Acción** en: **Reiniciar sistema**, **Apagar sistema** o **Realizar ciclo de encendido del sistema**, para que la opción **Pantalla de último bloqueo** funcione en el iDRAC6.
4. Haga clic en **Aplicar cambios**.
5. Para continuar, haga clic en el botón adecuado de la página **Servicios**. Vea la Tabla 21-13.

Tabla 21-6. Valores de configuración local

Valor	Descripción
Desactivar la configuración local del iDRAC por medio de la ROM de opción	Desactiva la configuración local del iDRAC por medio de la ROM de opción. La ROM de opción le pedirá que introduzca el módulo de configuración con la combinación de teclas <Ctrl+E> durante el reinicio del sistema.
Desactivar la configuración local del iDRAC por medio de RACADM	Desactiva la configuración local del iDRAC por medio de la RACADM de opción.

Tabla 21-7. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor web. Seleccionada=activado; deseleccionada=desactivado.
N° 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 **N.° máx. de sesiones**.
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 expiración actúan de inmediato y finalizan la sesión de interfaz web actual. Se debe restablecer el servidor web. Por favor espere unos minutos antes de abrir una sesión de interfaz web. El rango del tiempo de expiración es entre 60 y 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 de HTTPS	El puerto que el iDRAC utiliza para detectar una conexión de servidor. El valor predeterminado es **443**.

Tabla 21-8. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH Cuando está seleccionada, la casilla indica que SSH está activado.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango del tiempo de expiración es entre 60 y 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 21-9. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado.
Tiempo de	El tiempo de espera en inactividad del telnet, en segundos. El rango del tiempo de espera es de 60 a 1920. Introduzca 0 segundos para

espera	desactivar la función de tiempo de espera. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 21-10. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Cuando se verifica, la RACADM remota es activada.
Sesiones activas	El número de sesiones actuales en el sistema.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **N.º máx. de sesiones**.

Tabla 21-11. Configuración del agente SNMP

Valor	Descripción
Activado	Activa o desactiva el agente SNMP. Seleccionada=activado; deseleccionada=desactivado.
Nombre de comunidad	El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 21-12. Configuración del agente de recuperación automatizada del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automatizada del sistema.

Tabla 21-13. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

Activar 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 basada en web para activar estas funciones:

```
racadm config -g cfgRacTuning -o <nombre_de_objeto> <valor>
```

Además, use estas funciones en combinación con los valores correspondientes de 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 IpRange*) permite que sólo tengan acceso al iDRAC6 los clientes o estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Los demás inicios de sesión se rechazan.

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de **cfgRacTuning**:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propiedad **cfgRacTuneIpRangeMask** se aplica a la dirección IP entrante y a las propiedades **cfgRacTuneIpRangeAddr**. Si los resultados de ambas propiedades son idénticos, a la solicitud de inicio de sesión entrante se le concederá acceso al iDRAC6 Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión procederá si el valor de la siguiente expresión es igual a cero:

```
cfgRacTuneIpRangeMask & (<dirección_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

donde & es el operador Y a nivel de bits de las cantidades y ^ es el operador O exclusivo a nivel de bits.

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6." para ver una lista completa de las propiedades de **cfgRacTune**.

Tabla 21-14. Propiedades del filtrado de direcciones IP (IpRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación de rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Esta propiedad es una comparación con operador Y a nivel de bits con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6 Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el iDRAC6.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en forma de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior.

Activación del filtrado de IP

A continuación, se muestra un comando de ejemplo para la configuración del filtrado de IP.

Consulte "Uso de RACADM de manera remota" para obtener más información sobre RACADM y los comandos RACADM.

NOTA: Los siguientes comandos RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57)

Para restringir el inicio de sesión a una sola dirección IP (por ejemplo, 192.168.0.57), utilice toda la máscara, según se muestra a continuación.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Directrices para el filtrado de IP

Utilice las directrices a continuación cuando active el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Use la dirección base de rango que prefiera como el valor de **cfgRacTuneIpRangeAddr**. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits de orden inferior donde hay ceros en la máscara.

Bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el iDRAC6 durante un lapso de tiempo predefinido.

El parámetro de bloqueo de IP utiliza las funciones del grupo **cfgRacTuning** que incluyen:

- El número de intentos fallidos de inicio de sesión que se permiten
- El periodo en segundos dentro del que se deben presentar estos intentos fallidos
- La cantidad de tiempo en segundos que se impedirá que la dirección IP "responsable" establezca una sesión después de haber superado el número total permisible de intentos fallidos

Conforme se acumulan los intentos fallidos de inicio de sesión provenientes de una dirección IP específica, estos se "añejan" por medio de un contador interno. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: Identificación de intercambio de SSH: el host remoto cerró la conexión.

Consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6." para ver una lista completa de las propiedades de **cfgRacTune**.

La Tabla 21-15 muestra una lista de los parámetros definidos por el usuario.

Tabla 21-15. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presentan intentos fallidos consecutivos (**cfgRacTuneIpBlkFailCount**) provenientes de una misma dirección IP dentro de un periodo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecer una sesión que provengan de dicha dirección se rechazarán durante un periodo establecido (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El plazo en segundos dentro del que se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.
cfgRacTuneIpBlkPenaltyTime	Define el periodo en segundos dentro del que se rechazan todos los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Activación del bloqueo de IP

El ejemplo a continuación evita que una dirección IP cliente establezca una sesión durante cinco minutos cuando el cliente a tenido cinco intentos fallidos de inicio de sesión dentro de un periodo de un minuto.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente evita más de tres intentos fallidos dentro de un minuto y evita los intentos de inicio 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
```

Establecimiento de la configuración de la seguridad de red por medio de la interfaz gráfica de usuario del iDRAC6 GUI

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC6**

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Red**.
3. En la página **Configuración de red**, haga clic en **Configuración avanzada**.
4. En la página **Seguridad de la red**, configure los valores de los atributos y después haga clic en **Aplicar cambios**.

   La Tabla 21-16 describe los valores de la página **Seguridad de la red**.
5. Para continuar, haga clic en el botón adecuado de la página **Seguridad de la red**. Consulte la Tabla 21-17 para ver la descripción de los botones de la página **Seguridad de la red**.

Tabla 21-16. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango IP, que define un rango específico de direcciones IP que puede acceder al iDRAC6.
Dirección del rango de IP	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Este valor es bitwise AND'd con la Máscara de Subred del Rango IP para determinar la parte superior de una dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6 Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que

	un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el iDRAC6.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. Por ejemplo: **255.255.255.0**
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP.
Tiempo de penalización de bloqueo de IP	El periodo en segundos dentro del que se rechazan los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Tabla 21-17. Botones de la página de seguridad de la red

Botón	Descripción
Imprimir	Imprime la página **Seguridad de la red**
Actualizar	Vuelve a cargar la página **Seguridad de la red**
Aplicar cambios	Guarda los cambios que se hagan en la página **Seguridad de la red**.
Volver a la página de configuración de la red>	Regresa a la página **Configuración de la red**.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación básica de un iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección proporciona información sobre cómo instalar y configurar el hardware y software del DRAC6.

Antes de comenzar

Reúna los siguientes elementos que se incluyen con el sistema, antes de instalar y configurar el software del DRAC6:

- Hardware de DRAC6 (ya instalado o en el paquete opcional)
- Procedimeintos de instalación de iDRAC6 (incluídos en este capítulo)
- DVD *Dell Systems Management Tools and Documentation*

Instalación del hardware iDRAC6 Express/Enterprise

NOTA: La conexión del DRAC6 emula una conexión de teclado USB. Como resultado, cuando reinicie el sistema no notificará si el teclado no está conectado.

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

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

Configuración de su sistema para usar iDRAC6

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

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

sólo si la falla original en NIC 1 se ha corregido.

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

Generalidades de la instalación y configuración del software

Esta sección ofrece una descripción de alto nivel de la instalación del software del iDRAC6 y del proceso de configuración. Para obtener más información acerca de los componentes de software del DRAC6, consulte "Instalación del software en el sistema administrado".

Instalación del software del iDRAC6

Para instalar su software de iDRAC6:

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

Configuración de su iDRAC6

Para configurar su iDRAC6:

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

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

Instalación del software en el sistema administrado

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

Para instalar el software Managed System en el sistema administrado, utilice el DVD *Dell Systems Management Tools and Documentation*. Para obtener las instrucciones de cómo isntalar este software, vea la *Guía de Instalación Rápida* disponible en la página de soporte de Dell en **support.dell.com \ manuals**.

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

NOTA: No instale el Management Station de iDRAC6 ni el Managed System Software de iDRAC6 en el mismo sistema.

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

automática.

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

Instalación del software en la estación de administración

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

· La raíz del DVD root: incluye la Dell Systems Build and Update Utility, que proporciona la información de la configuración y sistema del servidor

· SYSMGMT: contiene productos de software de administración de sistemas incluyendo Dell OpenManage Server Administrator

· Docs: contiene documentación para productos de software de administración de sistemas, periféricos y controladores RAID

· SERVICIO: contiene las herramientas que necesita para configurar el sistema, y entrega los últimos diagnósticos y drivers optimizados por Dell para el sistema

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

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

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

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

Instalación de RACADM

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

   ```
   mount /media/cdrom
   ```

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

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

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

Desinstalación de RACADM

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

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

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

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

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

Actualización del firmware de iDRAC6

Utilice uno de los métodos siguientes para actualizar el firmware del DRAC6.

- Interfaz basada en la web (consulte "Actualización del firmware del iDRAC6 mediante la interfaz basada en web")
- CLI de RACADM)consulte "Actualización del firmware del iDRAC6 mediante RADCAM")
- Paquetes de actualización Dell (consulte "Actualización del firmware del iDRAC6 mediante paquetes de actualización de Dell para sistemas operativos Windows y Linux compatibles")

Antes de comenzar

Antes de actualizar el firmware del DRAC6 con RACADM local o Dell Update Packages, realice los siguientes procedimientos. De lo contrario, podría fallar la operación de actualización del firmware.

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

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

5. Compruebe que el USB esté activado.

Realice la carga del firmware iDRAC6

Para actualizar el firmware del DRAC6, descargue el firmware más reciente del sitio web de asistencia de Del que se encuentra en **support.dell.com** y guarde el archivo en el sistema local.

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

- Datos y código de firmware compilado del iDRAC
- Interfaz basada en 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 basada en web

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

Actualización del firmware del iDRAC6 mediante RADCAM

Puede actualizar el firmware del DRAC6 mediante la herramienta RACADM basada en CLI. Si ha instalado Server Administrator en el sistema administrado, utilice RACADM local para actualizar el firmware.

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

   Por ejemplo:

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

2. Ejecute el siguiente comando RACADM:

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

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

   Por ejemplo:

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

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

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

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

NOTA: Cuando actualice el firmware de iDRAC6 usando la utilería Update Package de Dellen Linux, podrá ver los siguientes mensajes en la consola:

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

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

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

Cómo borrar la caché del explorador

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

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

Configuración de un explorador de web admitido

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

Configuración del explorador de web para conectarse a la interfaz del iDRAC6 basada en web

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

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

1. Abra una ventana del explorador web.
2. Haga clic en **Herramientas** y haga clic en **Opciones de Internet**.
3. En la ventana **Opciones de Internet**, haga clic en la ficha **Conexiones**.
4. En **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
5. Si la casilla **Usar 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 DRAC6 por medio del explorador de web, se le pedirá agregar la dirección IP del DRAC6 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 de web para restablecer la conexión con la interfaz basada en web del DRAC6.

Exploradores de web de 32 bits y 64 bits

La interfaz basada en web del DRAC6 no se admite en los exploradores de web de 64 bits. Si abre un explorador de 64 bits, accede a la página de redirección de consola e intenta instalar el complemento, el procedimiento fallará. Si este error no se reconoce y se repite este procedimiento, la página de redirección de consola se cargará aun cuando la instalación del complemento haya fallado durante el primer intento. Este problema se presenta porque el explorador de web guarda la información del complemento en el directorio del perfil aun cuando el procedimiento de instalación del complemento haya fallado. Para resolver este problema, instale y ejecute un explorador web de 32 bits admitido e inicie sesión en iDRAC6.

Visualización de versiones localizadas de la interfaz basada en web

Windows

La interfaz basada en web del DRAC6 es compatible con los siguientes idiomas de sistemas operativos de Windows:

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

Para ver una versión traducida de la interfaz basada en web del DRAC6 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 redirección de consola en un cliente con Red Hat® Enterprise Linux® (versión 4) con interfaz gráfica en chino simplificado, es posible que el menú del visor y el título muestren caracteres aleatorios. Este problema se debe a una codificación incorrecta en el sistema operativo Red Hat Enterprise Linux (versión 4) en chino simplificado. Para resolver este problema, acceda a la configuración de codificación actual y modifíquela por medio de los siguientes pasos:

1. Abra una ventana de terminal de comandos.
2. Escriba "locale" y presione <Entrar>. Aparecerá el siguiente mensaje de salida.

   ```
   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:

   Anotación actual:

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

   Anotación actualizada:

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```
6. Cierre sesión y después inicie sesión en el sistema operativo.
7. Reinicie el iDRAC6.

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

Para ver las configuraciones avanzadas del DRAC6, consulte "Configuración avanzada del iDRAC6".

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del iDRAC6 por medio de la interfaz web

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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 de iDRAC6. Este capítulo proporciona información sobre cómo realizar tareas comunes de administración de sistemas con la interfaz Web de 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 Server-Management-Protocolo de Línea de Comandos. (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 núcleo al que se puede tener acceso de manera remota con una conexión Telnet o SSH. Para obtener mayor información sobre SM-CLP, consulte "Uso de la interfaz de línea de comandos de SM-CLP de iDRAC6." Para obtener mayor información sobre comandos RACADM consulte "Generalidades del subcomando RACADM" y "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

Acceso a la interfaz web

Para acceder a la interfaz Web de iDRAC6, realice los pasos que se indican a continuación:

1. Abra una ventana de un explorador web compatible.

   Consulte "Exploradores web admitidos" para obtener más información.

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

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

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

   En su navegador en la barra de **Dirección** escriba:

   https://<iDRAC-IPv4-address>

   Luego presione <Enter>.

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

   En su navegador en la barra de **Dirección** escriba:

   https://[<iDRAC-IPv6-address>]

   Luego presione <Enter>.

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

   https://<dirección_IP_de_iDRAC>:<número_de_puerto>

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

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

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

   https://*<dirección_IP_de_iDRAC>:<número_de_puerto>*

   donde *dirección_IP_de_iDRAC* es la dirección IP de iDRAC6 y *número_de_puerto* es el número del puerto HTTPS.

Aparecerá la ventana **Inicio de sesión** del iDRAC6.

Conexión

Puede iniciar sesión como usuario del iDRAC6 o como usuario de Microsoft® Active Directory®. El usuario predeterminado y contraseña para un usuario iDRAC6

son **root** y **calvin** respectivamente.

Para que pueda iniciar sesión en el iDRAC, el administrador debe haberle otorgado privilegio de **Inicio de sesión en el iDRA6.**

Para conectar, realice los pasos siguientes:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes valores:

   - Su nombre de usuario de 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>* *<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**, introduzca la contraseña de usuario del iDRAC6 o la contraseña de usuario de Active Directory. Las contraseñas distinguen entre mayúsculas y minúsculas.

3. Desde el casillero **Dominio**, seleccione *Este iDrac* para iniciar sesión como usuario de iDRAC6 o seleccione cualquier dominio disponuble para iniciar sesión como un usuario de Active Directory.

   NOTA: Para los usuarios de Active Directory, si usted tien un nombre de dominio específico como para del nombre de usuario, seleccione *Este iDRAC* desde el menú dropdown.

4. Haga clic en **Aceptar** o presione <Entrar>.

Desconexión

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 aparecerá a menos que usted haya iniciado sesión.

NOTA: Si cierra el explorador sin cerrar sesión de manera ordenada puede provocar que la sesión permanezca abierta hasta que se acabe el tiempo de espera. Se recomienda enfáticamente que haga clic en el botón de desconectar para terminar la sesión; de lo contrario, la sesión puede permanecer activa hasta que se acabe el tiempo de espera de la sesión.

NOTA: Cerrar la interfaz web de iDRAC6 en Microsoft Internet Explorer mediante el botón para cerrar ("x"), que se encuentra en la esquina superior derecha de la ventana, podría generar un error de aplicación. Para resolver este problema, descargue la actualización de seguridad acumulativa más reciente para Internet Explorer desde el sitio Web de asistencia de Microsoft, en **support.microsoft.com**.

Configuración de la NIC del iDRAC6

Esta sección supone que el iDRAC6 ya ha sido configurado y se puede tener acceso al mismo en la red. Consulte "Configuración de su iDRAC6" para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de LAN de IPMI y de red

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC**.

NOTA: La mayoría de los servidores DHCP requieren un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este símbolo durante la negociación de DHCP. El iDRAC6 proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

NOTA: Si usted utilizael Spanning Tree Protocol (STP) activado, asegúrese de que también tiene PortFast o una tecnología similar en funcionamiento de la siguiente forma:

- En los puertos para el interruptor conectados al iDRAC6
- En los puertos conectados a management station con una sesión del iDRAC KVM

  NOTA: Podría ver el siguiente mensaje si el sistema se detiene durante la autoprueba de encendido Precione la tecla F1 para continuar, F2 para ejecutar el programa de configuración del sistema.
  Una posible razón de error es un inconveniente de red que cause pérdida de comunicación con el iDRAC6. Después de que el inconveniente de red se solucione, reinicie el sistema.

  1. Haga clic en **Acceso Remoto**→ **Configuración**→ **Usuarios**.

  2. En la página **Red**, puede ingresar en las configuraciones de la tarjeta de interfaz de red, configuraciones comúnes de iDRAC, configuracionesIPv4, IPv6, IMPI y VLAN. Conslute Tabla 4-1, Tabla 4-2, Tabla 4-3, Tabla 4-4,

Tabla 4-5, y Tabla 4-6 para descripciones de esas propiedades.

3. Cuando haya terminado de introducir los valores necesarios, haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-7.

Tabla 4-1. Configuración de tarjeta de interfaz de red

Valor	Descripción
Selección de NIC	Configura el modo actual fuera de los modos posibles · Dedicado (iDRAC NIC) **NOTA:** Esta opción ya no está disponible en iDRAC6 Enterprise. · Compartido (Compartido con Failover todos controladores integrados de red.) Compartido con Failover todos controladores integrados de red. Compartido con Failover todos controladores integrados de red
MAC Address	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red.
Activar NIC	Cuando se selecciona, indica que el NIC está activado y habilita los controles restantes en este grupo. Cuando un NIC está desactivado, toda la comunicación hacia el iDRAC6 y que provenga del mismo a través de la red está bloqueada. El valor predeterminado es **activado**.
Negociar automáticamente	Si está **activado**, muestra la velocidad de red y modo al comunicarse con el router más cercano o hub. Si está **desactivado**, permite configurar la velocidad de red y el modo duplex en forma manual (desactivado) Si la Selección de la **NIC** *no* está **Dedicada**, la configuración de Negociación automática siempre estará **activada**.
Velocidad de red	Le permite configurar la velocidad de red a 100 Mb o 10 Mb para coincidir con su entorno de red. Esta opción no está disponible si **Negociación automática** se ha establecido como Activada.
Modo dúplex	Establezca el valor del modo dúplex en completo o medio para que coincida con el entorno de red. Esta opción no está disponible si **Negociación automática** se ha establecido como **Activada**.

Tabla 4-2. Configuraciones comúnes de iDRAC

Valor	Descripción
Registrar el iDRAC en DNS	Registra el nombre del iDRAC6 en el servidor DNS. El valor predeterminado es **Desactivado**.
Nombre DNS del iDRAC	Muestra el nombre del iDRAC6 únicamente cuando la opción **Registrar el iDRAC en DNS** está seleccionada. El nombre predeterminado es idrac-*etiqueta_de_servicio*, donde *etiqueta_de_servicio* es el número de la etiqueta de servicio del servidor Dell. Por ejemplo: idrac-00002
Usar DHCP para el nombre del dominio de DNS	Utiliza el nombre de dominio DNS predeterminado. Cuando la casilla no está seleccionada y la opción **Registrar el iDRAC en DNS** está seleccionada, usted puede modificar el nombre de dominio DNS en el campo **Nombre de dominio DNS**. El valor predeterminado es **Desactivado**. **NOTA:** Para seleccionar la casilla **Usar DHCP para el nombre del dominio DNS**, seleccione también la casilla **Usar DHCP (para la dirección IP de NIC)**.
Nombre del dominio DNS	El **nombre de dominio DNS** predeterminado está en blanco. Cuando la casilla **Usar DHCP para el nombre del dominio DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.

Tabla 4-3. Configuraciones de IPv4

Valor	Descripción
Activado	Si la NIC está activada, esto selecciona el soporte de protocolo IPv4 y establece los campos en este sección que se activarán.
Usar DHCP (Para la dirección IP de la tarjeta de interfaz de red)	Pide al iDRAC6 que obtenga una dirección IP para la NIC del servidor de Protocolo de configuración dinámica de host (DHCP). El valor predeterminado es **desactivado**.
Dirección IP	Especifica la dirección IP para la interfaz de red de la NIC del iDRAC
Máscara de subred	Permite ingresar o editar una dirección IP estática para el NIC del iDRAC6. Para cambiar este valor, deseleccione la casilla de marcación Usar DHCP (para dirección IP del NIC).

predeterminada	Dirección de un router o un interruptor. El valor se muestra en formato de números separados con puntos, por ejemplo, 192.168.0.1.
Usar DHCP para obtener direcciones de servidor DNS	Habilite el DHCP para obtener direcciones del servidor DNS por medio de la selección de la casilla **Use el DHCP para obtener direcciones de servidor DNS**. Cuando no se usa DHCP para obtener las direcciones del servidor DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**. El valor predeterminado es **apagado**. **NOTA:** Cuando la casilla **Use el DHCP para obtener direcciones de servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**.
Servidor DNS preferido	Dirección IP de servidor DNS
Servidor DNS alternativo	Dirección IP alternativa.

Tabla 4-4. Valores de IPv6

Valor	Descripción
Activado	Si la casilla está seleccionada IPv6 está activada Si la casilla no está seleccionada IPv6 está desactivada. El valor predeterminado es desactivado.
Auto Config	Verificar este casilla le permite al iDRAC6 obtener dirección IPv6 para la NIC del iDRAC6 desde el servidor del Protocolo de configuración dinámica de host (DHCP). Activar **Auto Config** también desactiva y hace salir los valores estáticos para dirección IP 1, longitud del prefijo y puerta de enlace IP.
IP Dirección 1	Especifica la dirección IPv6 para la interfaz de red de la NIC del iDRAC Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Longitud de prefijo	Configura la Longitud del Prefijo de la dirección IPv6.. Se puede valuar entre 1 y 128 inclusive. Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Puerta de enlace IP	Configura la puerta de enlace estática para la NIC del iDRAC Para cambiar esta configuración, primero debe desactivar **AutoConfig** quitando la selección de la casilla relacionada.
Dirección local de vínculo	Especifica la dirección IPv6 para la interfaz de red de la NIC del iDRAC
IP Dirección 2	Especifica la dirección adicional IPv6 address para el iDRAC NIC si una está disponible.
Usar DHCP para obtener direcciones de servidor DNS	Habilite el DHCP para obtener direcciones del servidor DNS por medio de la selección de la casilla **Use el DHCP para obtener direcciones de servidor DNS**. Cuando no se usa DHCP para obtener las direcciones del servidor DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**. El valor predeterminado es apagado. Verifique la copia de revisión Cuando la casilla **Use el DHCP para obtener direcciones de servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Especifica la dirección IPv6 estática del servidor DNS preferido. Para cambiar esta configuración, debe primero deseleccionar **Use el DHCP para obtener direcciones de servidor DNS**
Servidor DNS alternativo	Especifica la dirección IPv6 estática del servidor DNS alternativo Para cambiar esta configuración, debe primero deseleccionar **Use el DHCP para obtener direcciones de servidor DNS**

Tabla 4-5. Configuraciones de IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando está seleccionado, indica que el canal LAN de IPMI está activado. El valor predeterminado es **desactivadp**.
Límite del nivel de privilegios del canal	Configura el nivel máximo de privilegio del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: **Administrador**, **Operador** o **Usuario**. El valor predeterminado es **Administrador**.
Clave de cifrado	Configura la clave de cifrado: de 0 a 20 caracteres hexadecimales (no se permiten espacios). De manera predeterminada está en blanco.

Tabla 4-6. Configuraciones de VLAN

Valor	Descripción
Activar identificación de VLAN	Si está activada, solo tráfico ID de Virtual LAN (VLAN) será aceptado.
Identificación de VLAN	El campo de Id. de VLAN de campos de 802.1g. Un valor válido para la identificación de VLAN virtual debe ser un número entre 1 y 4094.
Prioridad	El campo Prioridad de campos de 802.1g. Ingrese un número entre 0 y 7 para establecer la prioridad del ID de VLAN

Tabla 4-7. Botones de la página de configuración de la red

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de red**.
Configuración avanzada	Abre la página **Seguridad de la red**, permitiendo al usuario ingresar atributos del rango de IP y de bloqueo de IP.
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la página de configuración de la red. **NOTA:** Si se hacen cambios en la configuración de la dirección IP de la NIC se cerrarán todas las sesiones de usuario y los usuarios tendrán que volver a conectarse a la interfaz Web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requerirán que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración de la filtración de IP y el bloqueo de IP

NOTA: Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el iDRAC**.

1. Haga click en **Acceso remoto**→ **Configuración** y luego en **Red** para abrir la nueva páginas de **Red**
2. Haga clic en **Configuración avanzada** para configurar los valores de seguridad de la red.

   La Tabla 4-8 describe los **valores de la página Seguridad de la red**. Cuando haya terminado de configurar los valores, haga clic en **Aplicar**.
3. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-9.

Tabla 4-8. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango de IP, que define un rango de direcciones IP que puede acceder al iDRAC. El valor predeterminado es **apagado**.
Dirección del rango de IP	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Este valor es bitwise AND'd con la Máscara de Subred del Rango IP para determinar la parte superior de una dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el iDRAC6 Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el iDRAC6.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. El valor predeterminado es **255.255.255.0**.
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido. El valor predeterminado es **apagado**.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección. El valor predeterminado es **10**.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. El valor predeterminado es **3600.**

Tabla 4-9. Botones de la página de seguridad de la red

Botón	Descripción
Imprimir	Imprime los valores de la **Seguridad de la red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Seguridad de la red**
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la página **Seguridad de la red**.
Regresa a la página Configuración de la red.	Regresa a la página **Configuración de la red**.

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 4-10.

Tabla 4-10. Filtros de eventos de plataforma

Índice	Suceso de plataforma
1	Declaración crítica del ventilador.
2	Declaración de advertencia de la batería
3	Declaración crítica de la batería
4	Declaración crítica de voltaje discreto
5	Declaración de advertencia de temperatura
6	Declaración crítica de temperatura
7	Declaración crítica de intrusión
8	Redundancia del ventilador degradada.
9	Redudancia del ventilador perdida.
10	Declaración de advertencia del procesador
11	Declaración crítica del procesador
12	Procesador ausente
13	Declaración de aviso del suministro de energía.
14	Declaración crítca del suministro de energía.
15	Suministro de energía ausente
16	Declaración crítica de registro de sucesos
17	Declaración crítica de vigilancia
18	Declaración de aviso de alimentación del sistema
19	Declaración crítica de aviso de alimentación del sistema

.

Cuando se presenta un suceso de plataforma (por ejemplo, la falla de una declaración de advertencia de la batería), se genera un suceso de sistema y se registra en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) que está activado y usted ha configurado el filtro para generar una alerta (PET o correo electrónico), se enviará una alerta por correo electrónico o captura de suceso de plataforma 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 ejecutará.

Configuración de los filtros de sucesos de plataforma (PEF)

NOTA: Configure los filtros de sucesos de plataforma antes de configurar capturas de sucesos de plataforma o alertas por correo electrónico.

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte "Acceso a la interfaz web".
2. Haga click en **Sistema**→ **Manejo de alertas**→ **Sucesos de plataforma**.
3. En la primera tabla, seleccione **Permitr alertas del filtro del suceso de platafoma** y luego haga click en **Aplicar cambios**.

   NOTA: Generar alerta deberá estar activado para que se envíe una alerta a cualquier destino válido configurado (PET o correo electrónico).
4. En la próxima tabla, **Lista de filtros de sucesos de plataforma**, haga click en el filtro que quiera configurar.
5. En la página **Configurar eventos de plataforma**, seleccione la **Acción de Apagado** Apropiada o seleccione **Ninguna**.
6. Seleccione o deseleccione **Generar Alerta** para activar o desactivar esta acción.

   NOTA: Generar alerta deberá estar activado para que se envíe una alerta a cualquier destino válido configurado (PET o correo electrónico).
7. Haga clic en **Aplicar cambios**.

   Ha regresado a la página **Sucesos de plataforma** donde los cambios que usted realizó se muestran en la **Lista de filtros de sucesos de plataforma.**
8. Repita los pasos del 4 al 7 para configurar filtros de sucesos de plataforma adicionales.

Configuración de capturas de suceso de plataforma (PET)

NOTA: Debe tener permiso para **Configurar el iDRAC** para poder agregar, activar o desactivar una alerta SNMP. Las opciones siguientes no estarán disponibles si usted no tiene permiso de **Configurar el iDRAC**.

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte "Acceso a la interfaz web".
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de sucesos de plataforma (PEF)".
3. Haga click en **Sistem→ Manejo de alertas→ Configuraciones de bloqueos**.
4. Tanto en la Lista de Destino **IPv4 o** la Lista de Destino **IPv6** haga click en el número de destino para configurar su destino de alerta SNMP de IPv4 o IPv6.
5. En la página **Configurar destino de alerta de suceso de plataforma**, seleccione o deseleccione **Activar destino**. Una casilla seleccionada indica que la dirección IP está activada para recibir las alertas. Una casilla no seleccionada indica que la dirección IP está desactivada para recibir las alertas.
6. Ingrese una dirección IP de destino de Bloqueo de Susceso de Plataforma Válida y haga click en **Aplicar cambios**.
7. Haga click en **Enviar el bloqueo de prueba** para verificar la alerta configurada o haga click en **Regresar a la página de destino de sucesos de plataforma.**

   NOTA: Su cuenta de usuario debe tener un permiso para **Verificar Alertas** para enviar un bloqueo de verificación. Conslute Tabla 6-6, "Permisos de grupos iDRAC Group Permissions," paaa mayor información.

   En la página **Destinos de alerta de sucesos de plataforma**, los cambios aplicados se muestran tanto en la **Lista de destino de IPv4 o IPv6.**
8. En el campo **Cadena de comunidad**, ingrese el nombre de comunidad SNMP del iDrac apropiado. Haga clic en **Aplicar cambios**.

   NOTA: La cadena de la comunidad de destino debe ser la misma que la cadena de la comunidad de iDRAC6.
9. Repita los pasos del 4 al 7 para configurar números de destino adicionales de IPv4 o IPv6.

Configuración de alertas por correo electrónico

NOTA: Alertas de correo electrónico que admiten tanto direcciones IPv4 y IPv6

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido.
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de sucesos de plataforma (PEF)".
3. Haga click en **Sistema→ Manejo de alerta→ Configuraciones de alertas de Email**.
4. En la tabla debajo de **Direcciones de correo electrónico. de destino**, haga click en **Número de alerta de correo electrónico** para la que quiere configurar la dirección de destino.
5. En la página **Configurar alerta de correo electrónico**, seleccione o deseleccione **Activar alerta de correo electrónico.** Una casilla seleccionada indica que la dirección IP está activada para recibir las alertas. Una casilla no seleccionada indica que la dirección IP está desactivada para recibir las alertas.
6. En el campo **Dirección de correo electrónico de destino**, escriba una dirección válida de correo electrónico.
7. En el campo **Descripción de correo electrónico**, escriba una breve descripción de lo que se mostrará en el correo electrónico.
8. Haga clic en **Aplicar cambios**
9. Si quiere verificar la alerta de correo electrónico configurada, haga click en **Enviar correo electrónico de prueba.**. Si no quiere, haga click en **Regresar a la página de destino de alertas de correo electrónico**
10. Haga click en **Regresar a la página de destino de alertas de correo electrónico** e ingrese una dirección IP de SMTP válida en el campo de dirección IP del servidor del.**SMTP (correo electrónicol)**

    NOTA: Para enviar un correo electrónico de prueba exitosamente, **la dirección IP del servidor SMTP (correo electrónico)** debe configurarse en la página **Configuraciones de alertas de correo electrónico.** El servidor SMTP utiliza la dirección IP establecida para comunicarse con el iDRAC6 para enviar alertas de correo electrónico cuando un suceso de plataforma ocurra.
11. Haga clic en **Aplicar cambios**
12. Repita los pasos del 4 al 9 para configurar destinos de alertas de correo electrónico adicionales.

Configuración de IPMI

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido.

2. Configure la IPMI en la LAN.

   a. En el árbol **Sistema**, haga clic en **Acceso remoto**.

   b. Haga clic en la ficha **Configuración** y haga clic en **Red**.

   c. En la página **Configuración de red** en **Configuración de LAN de IPMI**, seleccione **Activar IPMI en la LAN** y haga clic en **Aplicar cambios**.

   d. Actualice los privilegios del canal de LAN de IPMI, si es necesario.

   NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones IPMI 2.0.

   En **Configuración de LAN de IPMI**, haga clic en el menú desplegable **Límite de nivel de privilegios del canal**, seleccione **Administrador**, **Operador** o **Usuario** y haga clic en **Aplicar cambios**.

   e. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

   NOTA: La IPMI de iDRAC6es compatible con el protocolo RMCP+.

   En **Configuración de LAN de IPMI** en el campo **Clave de cifrado**, escriba la clave de cifrado y haga clic en **Aplicar cambios**.

   NOTA: La clave de cifrado debe consistir en un número par de caracteres hexadecimales con un máximo de 40 caracteres.

3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

   a. En el árbol **Sistema**, haga clic en **Acceso remoto**.

   b. En la ficha **Configuración**, haga clic en **Comunicación en serie en la LAN**.

   c. En la página **Configuración de la comunicación en serie en la LAN**, seleccione **Activar comunicación en serie en la LAN**.

   d. Actualice la velocidad en baudios de la SOL de IPMI.

   NOTA: Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

   e. Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

   f. Actualice el **Privilegio mínimo requerido.** Esta propiedad define el privilegio mínimo de usuario que se requiere para usar la función **Comunicación en serie en la LAN**.

   Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Usuario**, **Operador** o **Administrador**.

   g. Haga clic en **Aplicar cambios**.

4. Configure la conexión serie de IPMI.

   a. En la ficha **Configuración**, haga clic en **Serie**.

   b. En el menú **Configuración serie**, cambie el modo de la conexión serie de IPMI al valor adecuado.

   En **Conexión serie de IPMI**, haga clic en el menú desplegable **Valor del modo de conexión** y seleccione el modo adecuado.

   c. Establezca la velocidad en baudios de la conexión serie de IPMI.

   Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

   d. Establezca el límite del nivel de privilegios de canal.

   Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Administrador**, **Operador** o **Usuario**.

   e. Haga clic en **Aplicar cambios**.

   f. Compruebe que multiplexor serie esté configurado correctamente en el programa de configuración del BIOS del sistema administrado.

      - Reinicie el sistema.
      - Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
      - Diríjase a **Comunicación serie**.
      - En el menú **Conexión serie**, compruebe que **Conector serie externo** esté definido como **Dispositivo de acceso remoto**.
      - Guarde los cambios y salga del programa de configuración del BIOS.
      - Reinicie el sistema.

Si la conexión serie de IPMI está en modo de terminal, puede configurar los siguientes valores adicionales:

- Control de eliminación

- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0. Para información adicional acerca de comandos de modo terminal, consulte *Dell OpenManage Baseboard Management Controller Utilities User's Guide* en **support.dell.com\manuals**\.

Configuración de usuarios del iDRAC6

Para obtener más información, consulte "Cómo agregar y configurar usuarios del iDRAC6".

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales

Esta sección ofrece información sobre las funciones de seguridad de datos siguientes que vienen incorporadas en el iDRAC:

- Capa de conexión segura (SSL)
- Solicitud de firma de certificado (CSR)
- Acceder a SSL mediante interfaz basada en web
- Generación de una CSR
- Cómo cargar un certificado de servidor
- Cómo ver un certificado de servidor

Capa de conexión segura (SSL)

El iDRAC6 incluye un servidor web que está configurado para usar el protocolo de seguridad SSL -que es el estándar de la industria- para transferir datos cifrados a través de una red. Como está cimentado en la tecnología de cifrado de claves privada y pública, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autentificada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

- Se autentifique a sí mismo ante un cliente habilitado con SSL
- Permita que el cliente se autentifique a sí mismo ante el servidor
- Permita que ambos sistemas establezcan una conexión cifrada

El proceso de cifrado proporciona un alto nivel de protección de datos. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está generalmente disponible para los exploradores de Internet en Norteamérica.

De manera predeterminada, el servidor Web del iDRAC6 tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en la Internet, sustituya el certificado de SSL del servidor web con un certificado firmado por una autoridad reconocida de certificados. Para iniciar el proceso de obtención de un certificado firmado, se puede usar la interfaz Web del iDRAC6 para generar una solicitud de firma de certificado (CSR) con la información de la empresa. Usted podrá enviar entonces la CSR generada a una autoridad de certificados como VeriSign o Thawte.

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una CA para obtener un certificado de servidor seguro. Los certificados de servidor seguro hacen que los clientes del servidor confíen en la identidad del servidor al que se conectan y que negocien una sesión cifrada con el servidor.

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis fiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Una vez que la CA recibe una CSR, revisan y verifican la información que contiene la CSR. Si el solicitante cumple los estándares de seguridad de la CA, esta última emite un certificado firmado por medios digitales que identifica al solicitante de forma exclusiva para transacciones a través de redes y en la Internet.

Después de que la autoridad de certificados apruebe la CSR y envíe el certificado, cargue el certificado en el firmware del iDRAC6. La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información contenida en el certificado.

Acceder a SSL mediante interfaz basada en web

1. Hage click **en Acceso Remoto→ Configuración**

2. Haga clic en **SSL** para abrir la página **Menú principal de SSL**.

Use la página de **SSL** para realizar alguna de las siguientes acciones:

- Generar una Solicitud de firma de certificado (CSR)para enviar a una CA. La información de la CSR se almacena en el firmware del iDRAC6..
- Cargue un certificado del servidor.
- Vea un certificado del servidor.

Tabla 4-11 describe las opciones anteriores de la página **SSL**

Tabla 4-11.

Campo	Descripción
Solicitud de firma de certificado (CSR)	Esta opción le permite generar una CSR para enviar a una CA para solicitar un certificado web seguro. **NOTA:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la CA acepte la CSR, la CSR que está en el firmware debe coincidir con el certificado que la CA devuelve.
Cargar certificado de servidor	Esta opción le permite cargar un certificado existente sobre el que su compañía tenga derechos y que utiliza para controlar el acceso al iDRAC6. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509, base 64. No acepta certificados codificados DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su iDRAC6
Ver el certificado de servidor	Esta opción le permite ver un certificado de servidor existente.

SSL Opciones de página

Generación de una solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. Antes de que iDRAC pueda acetar su CSR firmado, la CSR en el firmware debe coincidir con el certificado que CA devuelve.

1. En la página **Menú principal d**e SSL, seleccione **Generar una nueva 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. Tabla 4-12 describe los atributos de la CSR
3. Haga click en **Generar** para crear la CSR y descargarla en su computera local.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-13.

Tabla 4-12. Opciones Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **www.empresaxyz.com**). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Tecnología informática). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo u otro carácter.
Nombre del estado:	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Texas). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Escriba la dirección de correo electrónico de la empresa o cualquier dirección de correo electrónico asociada con la CSR. Este campo es opcional.

Tabla 4-13. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime los valores de **Generar solicitud de firma de certificado** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Generar solicitud de firma de certificado**.

Generar	Genera una CSR y luego pide al usuario que lo guarde en un directorio específico.
Volver al menú principal de SSL	Regresa al usuario a la página **Menú principal de SSL**.

Carga de un certificado de servidor

1. En la página de **SSL**, seleccione **Cargar Certficado del Servidor** y seleccione **Siguiente**

   La página del **Certficado del Servidor cargado** aparece.

2. En el campo **Ruta de acceso del archivo**, escriba la ruta de acceso del certificado en el campo **Valor** o haga clic en **Examinar** para desplazarse hacia el archivo del certificado.

NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

3. Haga clic en **Aplicar**.

4. Haga clic en el botón correspondiente de la página para continuar. Vea la Tabla 4-14.

Tabla 4-14. Botones de la página de carga de certificados

Botón	Descripción
Imprimir	Vuelve a cargar la página **Carga del certificado**.
Volver al menú principal de SSL	Regresa a la página **Menú principal de SSL**.
Aplicar	Aplica el certificado al firmware del iDRAC6.

Cómo ver un certificado de servidor

1. En la página de **SSL**, seleccione **Muestrael Certficado del Servidor** y seleccione **Siguiente**.

   La página **Muestra el Certficado del Servidor**, visualiza el certificado del servidro que usted ha cargo al iDRAC.

   La Tabla 4-15 describe los campos asociados con las descripciones que aparecen en la tabla **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-16.

Tabla 4-15. Información de certificados

Campo	Descripción
Número de serie	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el sujeto
Información del emisor	Atributos del certificado generados por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de vencimiento del certificado

Tabla 4-16. Botones de página de visualización de certificados del servidor

Botón	Descripción
Imprimir	Imprime los valores de **Ver certificado del servidor** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Ver certificado del servidor**.
Volver al menú principal de SSL	Vuelve a la página de **SSL**

Configuración y administración de certificados de Active Directory

La página le permite configurar y gestionar las configuraciones de Active Directory

NOTA: Debe terner el permiso **Configurar iDRAC para usar o configurar** Active Directory.

NOTA: Antes de configurar o de usar la función de Active Directory, deberá asegurarse de que el servidor de Active Directory esté configurado para comunicarse con el iDRAC6..

NOTA: Para información más detallada sobre la configuración de Active Directory y como configurar Active Directory con un Esquema extendido o un Esquema Estándar, consulte"Uso de iDRAC6 con Microsoft Active Directory."

Para acceder a la página **Configuración y administración de Active Directory**.

1. Haga click **en Acceso Remoto→ Configuración**

2. Haga click en **Active Directory** para abrir la página de configuración y administración de **Active Directory**

   Tabla 4-17 describe las opciones de la página **Configuración y administración de Active Directory**.

3. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-18.

Tabla 4-17. Opciones de la página Configuración y administración de Active Directory

Atributo	Descripción
Valores comúnes	
Active Directory Activado	Especifica si Active Directory está activado o desactivado.
Selección de esquema	Especifica si el esquema estándar o extendido está en uso con Active Directory
Nombre de dominio del usuario	Este valor sostiene hasta 40 entradas de dominios de usuarios Si está configurada, la lista de nombres de dominios de usuarios aparecerá en las páginas de inicio como un menú pulldown para que el usuario que inicie sesión elija. Si no está configurada, los usuarios de Active Directory aún pueden iniciar sesión ingresando el nombre de usuario en el formato usuario_nombre@dominio_nombre, dominio_nombreusuario_nombre, o dominio_nombre\usuario_nombre.
Tiempo de espera	El tiempo en segundos de espera para que terminen las consultas a Active Directory. El valor predeterminado es 120 segundos.
Dirección del Servidor Controlador de Dominio 1-3 (FQDN o IP)	Especifica el nombre de dominio completo calificado (FQDN) del Controlador de Dominio o la dirección IP. Es necesario configurar al menos una de las 3 direcciones. iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. Si se selecciona esquema extendido, estas son las direcciones de los controladores de dominio donde el objeto dispositivo del iDRAC y los objetos de Asociación son localizados. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.
Validación del certificado activada.	iDRAC siempre utiliza el Protocolo de Acceso al Directorio Lightweight (LDAP) sobre Security Socket Layer (SSL) mientras se conecta a Active Directory De manera predeterminada, utiliza el CA certificado cargado en el iDRAC para validar el certificado del servidor del Cifrado de capa de conexión segura (SSL)de los controladores de dominio durante el cruce del Cifrado de capa de conexión segura (SSL) y proporciona fuerte seguridad. La validación del certificado se puede desactivar para verificar el propósito o el administrador del sistema elije confiar en los controladores de dominio en el límite de seguridad son validar sus certificados de Cifrado de capa de conexión segura (SSL) Esta opción especifica si la validación del Certificado está activada o desactivada..
Información del certificado de CA de Active Directory	
certificado	El certificado de la Autoridad de Certificados que firma el certificado del servidor Cifrado de capa de conexión segura (SSL) del controlador de dorminio.
Configuraciones del esquema extendido.	**Nombre del iDRAC:** Especifica el nombre que unicamente identifica 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.
Configuraciones de esquem estándar	**Dirección del Servidor del Catálogo Global 1-3 (FQDN or IP)**: Especifica el nombre de dominio calificado completo(FQDN) o la dirección IP del /los servidor(es) del Catálogo Global. Es necesario configurar al menos una de las 3 direcciones. iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. El servidor del Catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. **Grupos de funciones :** especifica la lista de grupos de función asociados al iDRAC6. **Nombre de grupo:** especifica el nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC6. **Dominio de grupo**: Especifica el dominio del grupo. **Privilegio del grupo**: nivel de privilegio para el grupo.

Tabla 4-18. Botones de la página Configuración y administración de Active Directory

Botón	Definición
Imprimir	Imprime los valores que se muestran en la página Configuración y administración de Active Directory
Actualizar	Vuelve a cargar la página Configuración y administración de Active Directory.
Configurar Active Directory	Le permite configurar Active Directory. Para obtener más información, consulte "Uso de iDRAC6 con Microsoft Active Directory".
Configuraciones de prueba	Permite que usted verifique la configuración de Active Directory con las configuraciones especificadas. Consulte"Uso de iDRAC6 con Microsoft Active Directory" para detalles la opción **Configuraciones de Prueba**.

Configuración de los servicios de iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

1. Haga click en **Acceso Remoto→ Configuración.** Luego, haga click en **Servicios** para mostrar el tipo de configuración de **Servicios.**
2. Configure los servicios siguientes según sea necesario:
   - Configuración local- ver Tabla 4-19
   - Servidor web: consulte la Tabla 4-20 para ver la configuración del servidor web
   - SSH: consulte Tabla 4-21 para ver la configuración de SSH
   - Telnet: consulte Tabla 4-22 para ver la configuración de Telnet
   - RACADM Remota-consultar Tabla 4-23 para ver la configuración de RACADM Remota.
   - Agente SNMP: consulte Tabla para obtener información sobre la configuración del agente SNMP
   - Agente de Recuperación del Sistema Automático (ASR)- consultar Tabla 4-25 para las configuraciones sobre el Agente ASR..
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 4-26.

Tabla 4-19. Configuración local ()

Valor	Descripción
Desactivar la configuración local del iDRAC por medio de la ROM de opcion	Desactiva la configuración local del iDRAC por medio de la ROM de opcion Option ROM se encuentro en el BIOS y proporciona un motor de interfaz del usuario que permite la configuración de iDRAC y BMC. La ROM de opción le pedirá que introduzca el módulo de configuración con la combinación de teclas <Ctrl+E> durante el reinicio del sistema.
Desactivar la configuración local del iDRAC por medio de RACADM	Desactiva la configuración local del iDRAC por medio de la RACADM de opción.

Tabla 4-20. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor Web del iDRAC6. Cuando está seleccionada, la casilla indica que el servidor web está activado. El valor predeterminado es **activado**.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Este campo no se puede editar. La cantidad máxima de sesiones simultáneas es 5..
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al N.° **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 expiración actúan de inmediato y finalizan la sesión de interfaz web actual. Se debe restablecer el servidor web. Por favor espere unos minutos antes de abrir una 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 en el que el iDRAC6 espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto de HTTPS	El puerto en el que el iDRAC6 espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 4-21. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH Cuando está seleccionada, la casilla indica que SSH está activado.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango del tiempo de espera es entre 60 y 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 4-22. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado.
Tiempo de espera	El tiempo de espera en inactividad del telnet, en segundos. El rango del tiempo de espera es de 60 a 1920. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **300**.
Número de puerto	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 4-23. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Cuando se verifica, la RACADM remota es activada.
Sesiones activas	El número de sesiones actuales en el sistema.

Tabla 4-24. Configuraciones de SNMP

Valor	Descripción
Activado	Activa/desactiva SNMP. Cuando se verifica, la SNMP remota es activada.
Nombre de comunidad SNMP	Activa/desactivae el nombre de comunidad SNMP Cuando se verifica, el nombre de comunidad SNMP se activa. El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 4-25. Configuración del agente de recuperación automatizada del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automatizada del sistema. Cuando se verifica, el Agente de Recuperación del Sistema Automático se activa.

Tabla 4-26. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

---

actualización del firmware de iDRAC6/de la imagen de recuperación de los servicios del sistema

NOTA: Si el firmware del iDRAC6 se daña, como puede suceder cuando el progreso de la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio de la interfaz Web del iDRAC6.

NOTA: De manera predeterminada, la actualización del firmware retendrá la configuración actual del iDRAC6. Durante el proceso de actualización, usted tiene la opción de restablecer los valores predeterminados de fábrica para la configuración del iDRAC6. Si establece la configuración a valores prederminados de fábrica,debe configurar la red utilizando la Utilidad de Configuraciónn del iDRAC6.

1. Abra la interfaz basada en web e inicie sesión en el sistema remoto.
2. Haga click en **Acceso remoto**, y luego en **Actualizar**.
3. En la página **Cargar/Descargar**(Paso 1 de 3) haga click en **Navegar** y escriba la dirección a la imagen del firmware que usted ha

descargado de **support.dell.com** o la imgen de recuperación de servicios del sistema.

NOTA: Si ejecuta Firefox, el cursor de texto no aparecerá en el campo **Imagen de firmware**.

Por ejemplo:

`C:\Updates\V1.0\<nombre_de_imagen>`.

O bien:

`\\192.168.1.10\Updates\V1.0\<imagen_nombre>`

El nombre predeterminado de la imagen de firmware es **firmimg.d6**.

4. Haga clic en **Cargar**.

   El archivo se cargará en el iDRAC6. Este proceso puede tardar varios minutos en completarse.

   El siguiente mensaje se mostrará hasta que el proceso se complete.

   `File upload in progress... (Carga de archivo en progreso...)`

5. En la página de **Estado (página 2 de 3)**, va a ver los resultados de la validación realizada sobre el archivo de imagen que usted cargó.

   - Si la imagen ha sido cargada exitosamente y aprobó todas las verificaciones, el nombre del archivo de imagen se mostrará. Si una imagen de firmware fue cargada, las versiones actuales y las nuevas de firmware se mostrarán.

     O bien:

   - Si la imagen no ha sido cargada exitosamente y no aprobó todas las verificaciones, un mensaje de error apropiado aparecerá y la actualización regresará a la página **Cargar/Descargar (Paso 1 de 3).** Puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

- Si es una imagen firmware, **Conservar configuración** le proporciona la opción de preservar o limpiar la configuración del iDRAC existente. Esta opción está seleccionada de forma predeterminada.

  NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada. Usted no podrá iniciar sesión en la interfaz Web del iDRAC6. Debe reconfigurar los valores de la LAN por medio de la utilidad de configuración del iDRAC6 durante la POST del BIOS.

7. Haga clic en **Iniciar actualización del firmware** para iniciar el proceso de actualización.

8. En la página de **Actualización (Paso 3 de 3)**, va a ver el estado de la actualización El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.

   NOTA: Mientras se encuentra en modo actulización, el proceso de actualización continuará detrás incluso si su navegador ya no se encuentra en este página.

   Si la actualización del firmware es exitosa, el iDRAC se reiniciará automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador. Se muetra un mensaje de error si se detecta algún error.

   Si la actualización del sistema de recuperación de servicios se completa/falla, un mensaje de estado apropiado aparecerá.

Reversión del firmware de iDRAC6

iDRAC6 debe mantener dos images de firmware simultáneas. Puede seleccionar reiniciar o (regresar) de la imagen de firmware seleccionada por usted.

1. Abra la interfaz basada en web e inicie sesión en el sistema remoto.

   Haga click en **Sistema→ Acceso remoto**, y luego en **Actualizar**.

2. En la página **Cargar/Regresar (Paso 1 de 3)**, haga click en **Regresar**. Las versiones de firmware actuales y anteriores se muestran en la página de **Estado (Paso 2 de 3).**

   Conservar configuración le proporciona la opción para conservar o limpiar la configuración del iDRAC existente. Esta opción está seleccionada de forma predeterminada.

   NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada. Usted no podrá iniciar sesión en la interfaz Web del iDRAC6. Deberá reconfigurar las configuraciones de la LAN utilizando la Utilidad de configuración durante BIOS POST o el comando racadm (localmente disponible en el servidor)

3. Haga clic en **Iniciar actualización del firmware** para iniciar el proceso de actualización.

   En la página de **Actualización** (Paso 3 de 3), va a ver el estado de la actualización El progreso, medido en porcentajes, aparecen en la columna **Progreso**.

NOTA: Mientras se encuentra en modo actulización, el proceso de actualización continuará detrás incluso si su navegador ya no se encuentra en este página.

Si la actualización del firmware es exitosa, el iDRAC se reiniciará automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador. Se muetra un mensaje de error si se detecta algún error.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración avanzada del iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección ofrece información sobre la configuración avanzada del iDRAC6. Su lectura se recomienda especialmente para los usuarios con conocimientos avanzados sobre la administración de sistemas que deseen personalizar el entorno de iDRAC6 de acuerdo con sus necesidades específicas.

Antes de comenzar

Usted debe haber terminado la instalación y configuración básica del hardware y software del iDRAC6. Consulte "Instalación básica de un iDRAC6" para obtener más información.

Configuración del iDRAC6 para visualizar la salida de la comunicación serial de forma remota a través de SSH/Telnet

Puede configurar el iDRAC6 para redireccionamiento remoto de la consola de comunicación serial siguiendo estos pasos:

Primero, configure el BIOS para permitir el redireccionamiento de la consola de comunicación serial:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   ```
   <F2> = System Setup (F2 = Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure las opciones en pantalla de la **Comunicación serie** como se indica a continuación:

   Comunicación serial....Activada con redireccionamiento serial a través de com2

   NOTA: Puede configurar la comunicación serial en **Activada con redireccionamiento serial a través de com1** siempre que el campo de dirección del puerto serial, dispositivo serial2, esté configurado en com1, también.

   Dirección del puerto serial....Dispositivo serial1 = com1, dispositivo serial2 = com2

   Conector serial externo....dispositivo serial1

   velocidad en baudios segura....115200

   tipo de terminal remota....vt100/vt220

   redireccionamiento después del inicio....Activado

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Configure los ajustes de iDRAC6 para activar SSH/Telnet

Luego, configure los ajuste de iDRAC6 para activar ssh/telnet, que puede realizar a través de RACADM o la interfaz web de iDRAC6.

Para cambiar la configuración de iDRAC6 para activar ssh/telnet usando RACADM, ejecute los comandos siguientes:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

También puede ejecutar los comandos RACADM remotamente; consulte "Uso de RACADM de manera remota."

Para cambiar la configuración de iDRAC6 para activar ssh/telnet usando la interfaz web de iDRAC6, siga estos pasos:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Servicios**.
3. Seleccione **Activar** en la sección **SSH** o **Telnet**.
4. Haga clic en **Aplicar cambios**.

El paso siguiente es conectarse a iDRAC6 usando Telnet o SSH.

Inicio de una consola de texto en Telnet o SSH

Después de haber iniciado sesión en el iDRAC6 a través del software de terminal de la estación de administración con Telnet o SSH, usted puede desviar la consola de texto del sistema administrado por medio de **console com2**, que es un comando de Telnet/SSH. Sólo se admite un cliente de **console com2** a la vez.

Para conectarse a la consola de texto de managed system, abra una línea de comando de iDRAC6 (a través de una sesión de telnet o SSH) y escriba:

```
console com2
```

El comando `console -h com2` muestra el contenido del búfer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serie.

El tamaño predeterminado (y máximo) del búfer de historial es de 8192 caracteres. Puede asignar un número menor a este valor con el comando:

```
racadm config -g cfgSerial -o cfgSerialHistorySize <número>
```

Para configurar Linux para direccionamiento de consola durante el inicio, consulte "Configuración de Linux para la redirección de la consola serie durante el inicio."

Uso de una consola de Telnet

Ejecutar Telnet usando Microsoft® Windows® XP o Windows 2003

Si la estación de administración está ejecutando Windows XP o Windows 2003, es posible que tenga un problema con los caracteres en las sesiones Telnet de iDRAC6. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla <Entrar> no responde y no aparece la petición de contraseña.

Para resolver este problema, descargue la revisión (hotfix) 824810 del sitio web de asistencia técnica de Microsoft en **support.microsoft.com**. Consulte el artículo 824810 de Microsoft Knowledge Base para obtener más información.

Ejecución de Telnet con Windows 2000

Si la estación de administración ejecuta Windows 2000, no se podrá acceder a la configuración del BIOS al presionar la tecla <F2>. Para resolver este problema, use el cliente Telnet que se incluye en la descarga gratuita recomendada de los servicios de Windows para UNIX® 3.5 de Microsoft. Vaya a **www.microsoft.com/downloads/** y busque "*Windows Services for UNIX 3.5*." (Servicios de Windows para UNIX 3.5).

Activación de telnet de Microsoft para redirección de consola telnet

NOTA: Es posible que algunos clientes Telnet en los sistemas operativos Microsoft no muestren correctamente la pantalla de configuración del BIOS cuando la redirección de la consola de BIOS está configurada para emulación de? VT100. Si se presenta este problema, cambie la redirección de la consola de BIOS al modo ANSI para actualizar la ventana. Para realizar este procedimiento en el menú de configuración del BIOS, seleccione **Redirección de consola** → **Tipo de terminal remota** → **ANSI**.

1. Active **Telnet** en **Servicios de componentes de Windows**.
2. Conéctese al iDRAC6 en la estación de administración.

   Abra un indicador de comandos, escriba lo siguiente y pulse <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 de Telnet (si se está usando un puerto nuevo).

Configuración de la tecla de retroceso para la sesión de Telnet

El uso de la tecla <Retroceso> puede producir resultados inesperados, según el cliente de Telnet. Por ejemplo, la sesión puede mostrar el eco ^h. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux se pueden configurar para usar la tecla <Retroceso>.

Para configurar los clientes Telnet de Microsoft para que utilicen la tecla <Retroceso>:

1. Abra una ventana de símbolo de sistema (si es necesario).
2. Si no está ejecutando una sesión de Telnet, escriba:

   `telnet`

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En el indicador, escriba:

   `set bsasdel`

   Aparece el mensaje siguiente:

   `Backspace will be sent as delete. (El retroceso se procesará como eliminación.)`

Para configurar una sesión de Telnet de Linux a fin de que utilice la tecla <Retroceso>:

1. Abra una petición de comandos y escriba:

   `stty erase ^h`
2. En el indicador, escriba:

   `telnet`

Uso de Secure Shell (SSH)

Es crucial que los dispositivos del sistema y la administración de dispositivos estén seguros. Los dispositivos incorporados y conectados son el centro medular de muchos procesos comerciales. Si estos dispositivos son vulnerables, la empresa puede estar en riesgo, lo que requiere de nuevas exigencias de seguridad al software de administración de dispositivos de CLI (interfaz de línea de comandos).

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 está activo en iDRAC6 cuando instala o actualiza el firmware de iDRAC6.

Se puede usar PuTTY u OpenSSH en la estación de administración para conectarse al iDRAC6 del sistema administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente Secure Shell envía un mensaje de error. El texto del mensaje depende del cliente y no es controlado por el iDRAC6.

NOTA: OpenSSH se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. La ejecución de OpenSSH en la petición de comandos de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

Sólo se admiten cuatro sesiones SSH a la vez. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se describe en "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6."

Para activar SSH en el iDRAC6, escriba:

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Para cambiar el puerto SSH, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>
```

Para obtener más información sobre las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

La implementación de SSH del iDRAC6 admite varios esquemas de criptografía, según se muestra en Tabla 5-1.

Tabla 5-1. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS 512:1024 bits (aleatorios) según la especificación NIST
Criptografía simétrica	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC

	• BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Integridad de mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autentificación	• Contraseña

NOTA: No se admite SSHv1.

Configuración de Linux para la redirección de la consola serie durante el inicio

Los pasos a continuación son específicos para GRand Unified Bootloader (GRUB) de Linux. Será necesario hacer cambios similares si se utiliza otro cargador de inicio.

NOTA: Cuando configure la ventana de emulación de cliente VT100, configure la ventana o aplicación que esté mostrando la consola redirigida en 25 filas x 80 columnas a fin de garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo **/etc/grub.conf** como se indica a continuación:

1. Localice las secciones General Setting (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=ttyS1,57600
   ```

3. Si el archivo **/etc/grub.conf** contiene una directiva splashimage, inserte un carácter de comentario al inicio de la línea para anularla.

La Tabla 5-2 contiene un ejemplo del archivo **/etc/grub.conf** que muestra los cambios que se describen en este procedimiento.

Tabla 5-2. Archivo de ejemplo: /etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0 console=ttyS1,57600
   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
```

```
(# 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 u 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
valor predeterminado=0
tiempo de espera=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
```

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial

título 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=ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
título Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im)
```

Cuando modifique el archivo **/etc/grub.conf**, aplique las siguientes directrices:

1. Desactive la interfaz gráfica de GRUB y utilice la interfaz de texto; de lo contrario, la pantalla de GRUB no aparecerá en la redirección de consola del RAC. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con `splashimage`.

2. Para activar varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión en serie del RAC, agregue la siguiente línea a todas las opciones:

   ```
   console=ttyS1,57600
   ```

   La Tabla 5-2 muestra la cadena `console=ttyS1,57600` ya agregada a la primera opción solamente.

Activación del inicio de sesión en la consola después de inicio

Modifique el archivo **/etc/inittab** según se indica a continuación:

Agregue una nueva línea para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

La Tabla 5-3 muestra un archivo de ejemplo con la nueva línea.

Tabla 5-3. Archivo de ejemplo: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

```
(#
# 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
```

```
# 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 nuestro UPS 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 potencia instalada y que el
# UPS está conectado 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"
```

```

# 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
```

Configuración de iDRAC6 para conexión serial

Puede usar cualquiera de las interfaces siguientes para conectarse a iDRAC6 a través de una conexión serial:

- CLI de iDRAC6
- Modo básico de conexión directa
- Modo de terminal de conexión directa

Para configurar su sistema para usar cualquiera de estas interfaces, realice los pasos siguientes.

Configure el **BIOS** para activar conexiones seriales:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   ```
   <F2> = System Setup (F2 = Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure la pantalla **Comunicación serie** como se indica a continuación:

   Conector serie externo....dispositivo de acceso remoto

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Luego, conecte el cable DB-9 o Nulo del modem de la estación de administración al servidor administrado en nodo. Consulte "Conexión del cable nulo de módem o DB-9 para la consola serial".

Posteriormente, asegúrese de que el software emulador de terminal de administración esté configurado para conexiones seriales. Consulte "Configuración del software de emulación de terminal de la estación de administración".

Luego, configure los ajuste de iDRAC6 para activar conexiones seriales, que puede realizar a través de RACADM o la interfaz web de iDRAC6.

Para cambiar la configuración de iDRAC6 para activar conexiones seriales usando RACADM, ejecute el comando siguiente:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Para cambiar la configuración de iDRAC6 para activar conexiones seriales usando la interfaz web de iDRAC6, siga estos pasos:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. Seleccione **Activado** en la sección **RAC Serial**.
4. Haga clic en **Aplicar cambios**.

Cuando ha establecido una conexión serial con la configuración anterior, deberá ver una solicitud de contraseña. Ingrese el nombre de usuario y contraseña de iDRAC6 (los valores predeterminados son `root` y `calvin`, respectivamente).

Desde esta interfaz, puede ejecutar varias funciones como RACADM. Por ejemplo, para imprimir el Registro de eventos del sistema, ingrese el siguiente comando RACADM:

```
racadm getsel
```

Configuración de iDRAC para el Modo básico de conexión directa y Modo de terminal de

conexión directa

Usando RACADM, ejecute el siguiente programa para desactivar la interfaz de línea de comandos de 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 de iDRAC6:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. Deseleccione **Activado** en la sección **RAC Serial**.

   Para el Modo básico de conexión directa:

   En la sección **IPMI Serial** cambie la opción del menú desplegable **Configuración del modo de conexión** a **Modo básico de conexión directa**.

   Para el Modo de terminal de conexión directa

   En la sección **IPMI Serial** cambie la opción del menú desplegable **Configuración del modo de conexión** a **Modo de terminal de conexión directa**.
4. Haga clic en **Aplicar cambios**. Para obtener más información sobre los Modos básico y de terminal de la conexión directa, vea "Configuración de los modos serie y terminal."

El Modo básico de conexión directa le permitirá usar herramientas como ipmish directamente a través de la conexión serial. Por ejemplo, para imprimir el Registro de eventos del sistema usando ipmish a través del modo Básico de IPMI, ejecute el comando siguiente:

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
```

El modo de terminal de conexión directa le permitirá enviar comandos ASCII al iDRAC6. Por ejemplo, para encender/apagar el servidor a través del modo de terminal de conexión directa:

1. Conéctese a iDRAC6 por medio del software de emulación de terminal
2. Escriba el comando siguiente para iniciar sesión:

   ```
   [SYS PWD -U root calvin]
   ```

   Verá la respuesta siguiente:

   ```
   [SYS]

   [OK]
   ```
3. Escriba el comando siguiente para verificar un inicio de sesión exitoso:

   ```
   [SYS TMODE]
   ```

   Verá la respuesta siguiente:

   ```
   [OK TMODE]
   ```
4. Para apagar el servidor (el servidor se apagará inmediatamente), escriba el comando siguiente:

   ```
   [SYS POWER OFF]
   ```
5. Para encender el servidor (el servidor encenderá inmediatamente):

   ```
   [SYS POWER ON]
   ```

Conmutación entre el Modo de terminal de conexión directa y el redireccionamiento de la consola serial

iDRAC6 admite secuencias de la tecla Escape que permiten la conmutación entre el modo de terminal de conexión directa y el redireccionamiento de la consola serial.

Para configurar el sistema para que admita ese comportamiento, siga estos pasos:

1. Encienda o reinicie el sistema.
2. Oprima <F2> inmediatamente después de ver el siguiente mensaje:

   ```
   <F2> = System Setup (F2 = Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure la pantalla **Comunicación serie** como se indica a continuación:

   comunicación serial -- Activada con redireccionamiento serial a través de com2

   NOTA: Puede configurar el campo de **comunicación serial** a **Activado con redireccionamiento a través de com1** siempre que **dispositivo serial2** en el campo de la **dirección del puerto serial** también esté configurado en com1.

   Dirección del puerto serial -- Dispositivo serial1 = com1, dispositivo serial2 = com2

   Conector serial externo -- dispositivo serial2

   velocidad en baudios segura....115200

   tipo de terminal remota ...vt100/vt220

   redireccionamiento después del inicio ... Activado

   Luego, seleccione **Guardar cambios**.

5. Presione <Esc> para salir del programa **Configuración de sistema** y terminar la configuración del mismo.

Para cambiar al Modo de redireccionamiento de consola serial cuando esté en el Modo de terminal de la conexión directa, use la siguiente secuencia de la tecla Escape:

<Esc> +<Mayús> <q>

Para cambiar al Modo de terminal de la conexión directa cuando esté en el Modo de la redireccionamiento de consola serial, use la siguiente secuencia de la tecla Escape:

<Esc> +<Mayús> <9>

Conexión del cable nulo de módem o DB-9 para la consola serial

Para acceder al sistema administrado con una consola de texto serie, conecte un cable de módem nulo DB-9 al puerto COM del sistema administrado. Co0n objeto de que la conexión funcione con el cable de modem NULO, se deberán realizar las configuraciones correspondientes de comunicaciones seriales en la configuración de CMOS. No todos los cables DB-9 tienen la distribución de patillas/señales necesaria para esta conexión. El cable DB-9 de esta conexión debe cumplir las especificaciones que se muestran en la Tabla 5-5.

NOTA: El cable DB-9 también se puede usar para la redirección de consola de texto de BIOS.

Tabla 5-5. Distribución de patillas necesaria para el cable de módem nulo DB-9

Nombre de señal	Patilla DB-9 (patilla de servidor)	Patilla DB-9 (patilla de estación de trabajo)
FG (protección de tierra)	-	-
TD (transmisión de datos)	3	2
RD (recepción de datos)	2	3
RTS (solicitud de envío)	7	8
CTS (listo para envío)	8	7
SG (señal de tierra)	5	5
DSR (conjunto de datos listo)	6	4
CD (detección de transportador)	1	4
DTR (terminal de datos listo)	4	1 y 6

Configuración del software de emulación de terminal de la estación de administración

El iDRAC6 admite una consola de texto telnet o serie de una estación de administración que ejecute uno de los siguientes tipos de software de emulación de

terminal:

- Linux Minicom en Xterm
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve
- Linux Telnet en Xterm
- Microsoft Telnet

Realice los pasos en los apartados siguientes para configurar el tipo del software de terminal. Si está usando Microsoft Telnet, no se requiere la configuración.

Configuración de Linux Minicom para la emulación de consola serie

Minicom es la utilidad de acceso a puerto serie de Linux. Los pasos siguientes son válidos para configurar Minicom versión 2.0. Otras versiones de Minicom pueden diferenciarse ligeramente, pero requieren los mismos valores básicos. Utilice la información en "Valores de Minicom necesarios para la emulación de consola serie" para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0 para emulación de la consola serie

NOTA: Para garantizar que el texto se muestre correctamente, Dell recomienda que se utilice una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece el sistema Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en la petición de comandos.
2. En la ventana de Xterm, lleve la flecha del 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 luego vaya al paso 17.
4. En la petición de comandos de Xterm, escriba `minicom -s`.
5. Seleccione **Serial Port Setup** (Configuración de puerto serie) y pulse <Entrar>.
6. Presione <a> y seleccione el dispositivo serie correspondiente (por ejemplo, **/dev/ttyS0**).
7. Presione <e> y establezca la opción **Bps/Par/Bits** en **57600 8N1**.
8. Presione <f> y establezca **Control de flujo de hardware** en **Sí** y **Control de flujo de software** en **No**.
9. Para salir del menú **Configuración del puerto serie**, presione <Entrar>.
10. Seleccione **Módem y marcación** y presione <Entrar>.
11. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco.
12. Presione <Entrar> para guardar cada uno de los valores en blanco.
13. Cuando se hayan borrado todos los campos especificados, presione <Entrar> para salir del menú **Configuración de parámetros y marcación de módem**.
14. Seleccione **Guardar configuración como nombre_de_config** y presione <Entrar>.
15. Seleccione **Salir de Minicom** y presione <Entrar>.
16. En la petición del intérprete de comandos, escriba `minicom <nombre` *`del archivo de configuración de Minicom`*>.
17. Para ampliar la ventana de Minicom a 80 x 25, arrastre la esquina de la misma.
18. Presione <Ctrl+a>, <z>, <x> para salir de Minicom.

NOTA: Si utiliza Minicom para la redirección de consola de texto serie para configurar el BIOS del sistema administrado, se recomienda activar el color en Minicom. Para activar el color, escriba el comando siguiente: `minicom -c on`

Asegúrese de que la ventana Minicom muestre una petición de comando. Cuando la petición de comandos aparezca, la conexión se habrá establecido satisfactoriamente y usted estará listo para conectarse a la consola del sistema administrado por medio del comando serie **connect**.

Valores de Minicom necesarios para la emulación de consola serie

Utilice la Tabla 5-6 para configurar cualquier versión de Minicom.

Tabla 5-6. Valores de Minicom para emulación de consola serie

Descripción del valor	Valor necesario
Bps/Par/Bits	57600 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Marcación de módem y configuración de parámetros	Borre los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco
Tamaño de ventana	80 x 25 (para cambiar el tamaño, arrastre la esquina de la ventana)

Configuración de HyperTerminal para la redirección de consola serie

HyperTerminal es la utilidad de acceso de puerto serie de Microsoft Windows. Para establecer el tamaño de la pantalla de consola correctamente, utilice HyperTerminal Private Edition versión 6.3 de Hilgraeve.

Para configurar HyperTerminal para la redirección de consola serie:

1. Inicie el programa HyperTerminal.
2. Escriba un nombre para la nueva conexión y haga clic en **Aceptar**.
3. Junto a **Conectar usando:**, seleccione el puerto COM en la estación de administración (por ejemplo, COM2) al que ha conectado el cable de módem nulo DB-9 y haga clic en **Aceptar**.
4. Configure los valores del puerto COM según se muestra en la Tabla 5-7.
5. Haga clic en **OK** (Aceptar).
6. Haga clic en **Archivo** → **Propiedades** y después haga clic en la ficha **Configuración**.
7. Defina la **Id. de la terminal de Telnet:** como **ANSI**.
8. Haga clic en **Configuración de terminal** y establezca **Filas de pantalla** en **26**.
9. Establezca **Columnas** en **80** y haga clic en **Aceptar**.

Tabla 5-7. Configuración del puerto COM de la estación de administración

Descripción del valor	Valor necesario
Bits por segundo	57600
Bits de datos	8
Paridad	Ninguno
Bits de parada	1
Control de flujo	Hardware

Configuración de los modos serie y terminal

Configuración de la conexión serie de IPMI y iDRAC6

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. Configurar los valores de conexión serie de IPMI.

Consulte la Tabla 5-8 para ver una descripción de los valores de la conexión serie de IPMI.

4. Configurar los valores de conexión serie de iDRAC6.

   Consulte Tabla 5-9 para ver una descripción de los valores de la conexión serie de iDRAC6.

5. Haga clic en **Aplicar cambios**.

6. Haga clic en el botón adecuado de la página **Configuración serie** para continuar. Consulte la Tabla 5-10 para ver una descripción de los valores de la página de configuración de la conexión serie.

Tabla 5-8. Configuración de la conexión serie de IPMI

Valor	Descripción
Configuración del modo de conexión	• Modo básico de conexión directa: Modo básico de conexión serie de IPMI • Modo de terminal de conexión directa: Modo de terminal de conexión serie de IPMI
Velocidad en baudios	• Establece la velocidad de los datos. Seleccione **9600 bps**, **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.
Control de flujo	• Ninguno: Control de flujo de hardware apagado • RTS/CTS: Control de flujo de hardware encendido
Límite del nivel de privilegios del canal	• Administrador • Operador: • Usuario

Tabla 5-9. Valores de configuración de iDRAC6

Valor	Descripción
Activado	Activa o desactiva la consola serie de iDRAC6. Seleccionada=activada; deseleccionada=desactivada
Tiempo de espera	La cantidad máxima de segundos de línea disponible antes de que la línea 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 redirección de consola. Seleccionada=activada; deseleccionada=desactivada
Velocidad en baudios	La velocidad de los datos en el puerto serie externo. Los valores son **9600 bps**, **28,8 kbps**, **57,6 kbps** y **115,2 kbps**. El valor predeterminado es de **57,6 kbps**.
Tecla Escape	Especifica la tecla <Esc>. El valor predeterminado son los caracteres ^\.
Tamaño del búfer de historial	El tamaño del búfer de historial de la conexión serie, que guarda los últimos caracteres que se escribieron en la consola. El valor máximo y predeterminado es 8192 caracteres.
Comando de inicio de sesión	La línea de comando del iDRAC6 que se ejecutará ante un inicio de sesión válido.

Tabla 5-10. Valores de la página de configuración de la conexión serie

Botón	Descripción
Imprimir	Imprime la página **Configuración de la conexión serie**.
Actualizar	Actualiza la página **Configuración de la conexión serie**.
Aplicar cambios	Aplica los cambios de la conexión serie de iDRAC6 e IPMI.
Configuración del modo de terminal	Abre la página **Configuración del modo de terminal**.

Configuración del modo de terminal

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.

2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.

3. En la página **Configuración de la conexión serie**, haga clic en **Configuración del modo de terminal**.

4. Defina la configuración del modo de terminal.

   Consulte la Tabla 5-11 para ver una descripción de la configuración del modo de terminal.

5. Haga clic en **Aplicar cambios**.

6. Haga clic en el botón correspondiente de la página **Configuración del modo de terminal** para continuar. Consulte la Tabla 5-12 para ver una descripción de los botones de la página de configuración del modo de terminal.

Tabla 5-11. Configuración del modo de terminal

Valor	Descripción
Edición de línea	Activa o desactiva la edición de línea.
Control de eliminación	Selecciona una de las siguientes opciones: • **El iDRAC6 genera un carácter <retroceso><espacio><retroceso> cuando se recibe <retroceso> o <supr>**. • **El iDRAC6 genera un carácter <supr> cuando se recibe <retroceso> o <supr>**.
Control del eco	Activa o desactiva el eco.
Control del protocolo de enlace	Activa o desactiva el protocolo de enlace.
Nueva secuencia de línea	Selecciona **Ninguno**, **<CR-LF>**, **<NULO>**, **<CR>**, **<LF-CR>** o **<LF>**.
Introducir una nueva secuencia de línea	Seleccione **<CR>** o **<NULO>**.

Tabla 5-12. Botones de la página de configuración del modo de terminal

Botón	Descripción
Imprimir	Imprime la página **Configuración del modo de terminal**.
Actualizar	Actualiza la página **Configuración del modo de terminal**.
Regresar a la configuración del puerto serie	Regresa a la página **Configuración del puerto serie**.
Aplicar cambios	Aplica los cambios de la configuración del modo de terminal.

Configuración de los valores de la red de iDRAC6

PRECAUCIÓN: Si cambia la configuración de red del iDRAC6, podría provocar que su conexión de red actual se desconecte.

Configure los valores de red del iDRAC6 con una de las herramientas siguientes:

- Interfaz web: consulte "Configuración de la NIC del iDRAC6"
- CLI de RACADM: consulte "cfgLanNetworking"
- Utilidad de configuración del iDRAC6: consulte "Configuración de su sistema para usar iDRAC6"

NOTA: Si va a instalar el iDRAC6 en un entorno de Linux, consulte "Instalación de RACADM".

Acceso al iDRAC6 a través de una red

Después de configurar el iDRAC6, usted puede acceder de manera remota el sistema administrado por medio de una de las interfaces siguientes:

- Interfaz basada en web
- RACADM
- Consola Telnet
- SSH
- IPMI

Tabla 5-13 describe cada interfaz de iDRAC6.

Tabla 5-13. Interfaces iDRAC6

Interfaz	Descripción
Interfaz basada en web	Proporciona acceso remoto al iDRAC6 por medio de una interfaz gráfica para el usuario. La interfaz web está integrada en el firmware del iDRAC6 y se accede a ella por medio de la interfaz de NIC a partir de un explorador de web compatible de la estación de administración. Para ver una lista de los exploradores de web admitidos, consulte "Exploradores web admitidos".

RACADM	Ofrece acceso remoto al iDRAC6 por medio de una interfaz de línea de comandos. RACADM usa la dirección IP de iDRAC6 para ejecutar comandos RACADM. **NOTA:** La opción de capacidad remota de racadm sólo se admite en las estaciones de administración. Para obtener más información, consulte "Uso de RACADM de manera remota". **NOTA:** Al utilizar la capacidad remota de racadm, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo: `racadm getconfig -f <nombre de archivo>` o bien: `racadm sslcertupload -t 1 -f c:\cert\cert.txt subcomandos`
Consola Telnet	Proporciona acceso a iDRAC6 y soporte para los comandos seriales y RACADM, incluyendo los comandos **powerdown**, **powerup**, **powercycle**, y **hardreset**. **NOTA:** Telnet es un protocolo no seguro que transmite todos los datos -incluso las contraseñas- en texto simple. Cuando transmita información confidencial, utilice la interfaz SSH.
Interfaz SSH	Proporciona las mismas capacidades que la consola Telnet a través de una capa de transporte cifrada que brinda mayor seguridad.
Interfaz IPMI	Brinda acceso a las funciones de administración básicas del sistema remoto por medio del iDRAC6. La interfaz incluye IPMI mediante LAN, IPMI mediante conexión serie y Conexión serie mediante LAN. Para obtener más información, consulte la *Guía del usuario Dell OpenManage Baseboard Management Controller Utilities* 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 basada en web del iDRAC6 mediante el NIC del iDRAC6, utilizando un explorador de web admitido o mediante Server Administrator o IT Assistant.

Consulte "Exploradores web admitidos" para ver una lista de los exploradores de web admitidos.

Para acceder a la interfaz de acceso remoto del iDRAC6 por medio de Server Administrator, ejecute Server Administrator. En el árbol de sistema que se encuentra en el panel a la izquierda de la página de inicio de Server Administrator, haga clic en **Sistema** → **Chasis del sistema principal** → **Controlador de acceso remotor**. Para obtener más información, consulte la guía del usuario de Server Administrator.

Uso de RACADM de manera remota

NOTA: Configure la dirección IP en el iDRAC6 antes de usar la capacidad remota de RACADM. Para obtener más información sobre cómo configurar el iDRAC6 y una lista de los documentos relacionados, consulte "Instalación básica de un iDRAC6".

RACADM proporciona una opción de capacidad remota (**-r**) que le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para usar la capacidad remota, usted necesita un nombre de usuario válido (opción -u) y una contraseña (opción -**p**), así como la dirección IP del iDRAC6.

NOTA: Si el sistema desde el que está accediendo al sistema remoto no tiene un certificado de iDRAC6 en el almacén predeterminado de certificados, aparecerá un mensaje cuando escriba un comando de RACADM. Para obtener más información sobre los certificados de iDRAC6, consulte "Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales".

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (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)

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors. (Ejecución continua. Utilice la opción
-S para que racadm detenga la ejecución al producirse errores relacionados con certificados.)
```

RACADM continúa ejecutando el comando. No obstante, si utiliza la opción –S, RACADM detendrá la ejecución del comando y mostrará el siguiente mensaje:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (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 not continuing execution of the command. (Racadm detiene la ejecución del comando.)
```

ERROR: no es posible establecer conexión con el iDRAC6 en la dirección IP especificada

NOTA: La capacidad remota de RACADM sólo se admite en las estaciones de administración. Para obtener más información, consulte la *matriz de compatibilidad de software de los sistemas Dell* que se encuentra en la sección **OpenManage Software de Dell** en el sitio web de asistencia de Dell en **support.dell.com\manuals**.

NOTA: Al utilizar la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo:

```
racadm getconfig -f <nombre de archivo>
```

O bien:

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt subcomandos
```

Sinopsis de RACADM

```
racadm -r <dirección IP del iDRAC6 > -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6 > <subcomando> <opciones del subcomando>
```

Por ejemplo:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del iDRAC6 se ha cambiado a un puerto personalizado diferente al puerto predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP del iDRAC6>:<puerto> -u <nombre_de_usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6>:<puerto> <subcomando> <opciones del subcomando>
```

Opciones de RACADM

La Tabla 5-14 muestra una lista de las opciones del comando RACADM.

Tabla 5-14. Opciones del comando racadm

Opción	Descripción
-r <*Direc_IP_de_RAC*> **-r <*Direc_IP_de_RAC*>:<*número de puerto*>**	Especifica la dirección IP remota del controlador. Use <*número de puerto*> si el número de puerto del iDRAC6 no es el puerto predeterminado (443)
-i	Indica a RACADM que pregunte interactivamente al usuario el nombre de usuario y la contraseña.
-u <*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 de RACADM remota está activada de manera predeterminada. Si se desactiva, escriba el siguiente comando de RACADM para activarla:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

Para desactivar la capacidad remota, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

Subcomandos de RACADM

Tabla 5-15proporciona la descripción de cada uno de los subcomandos de RACADM que se puede ejecutar en RACADM. Para ver una lista detallada de los subcomandos de RACADM que incluye la sintaxis y las anotaciones válidas, consulte "Generalidades del subcomando RACADM".

Al introducir un subcomando de RACADM, preceda el comando con racadm, por ejemplo.

```
racadm help
```

Tabla 5-15. Subcomandos de RACADM

Comando	Descripción
help	Lista los subcomandos iDRAC6.

help *<subcomando>*	Muestra la descripción de uso del subcomando especificado.
arp	Muestra el contenido de la tabla de ARP. Las anotaciones del ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la pantalla de último ASR (bloqueo) (la última pantalla azul).
clrraclog	Borra el registro iDRAC6. Sólo se hace una 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 de iDRAC6.
coredumpdelete	Borra el volcado del núcleo almacenado en 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 el tiempo de iDRAC6.
ifconfig	Muestra la configuración actual de IP 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 para el controlador.
getniccfg	Muestra la configuración IP actual del controlador.
getsvctag	Muestra las etiquetas de servicio.
racdump	Vacía información del estado y la condición del iDRAC6 para la depuración de errores.
racreset	Restablece el iDRAC6.
racresetcfg	Restablece la configuración predeterminada del iDRAC6.
serveraction	Realiza operaciones de administración de energía en el sistema administrado.
getraclog	Muestra el registro de 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 de 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 CA.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el iDRAC6.
sslkeyupload	Obliga al iDRAC6 a enviar un mensaje de correo electrónico de prueba a través del NIC del iDRAC6 para comprobar la configuración de correo electrónico.
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.
vmkey	Restablece el tamaño predeterminado de la memoria flash virtual (256 MB).

Preguntas frecuentes sobre los mensajes de error de RACADM

Tras realizar un restablecimiento del iDRAC6 (con el comando racadm racreset), escribo un comando y aparece el mensaje siguiente:

ERROR: Unable to connect to RAC at specified IP address (ERROR: no es posible establecer conexión con el RAC en la dirección IP especificada)

¿Qué significa este mensaje?

Debe esperar hasta que el iDRAC6 haya completado el restablecimiento antes de ejecutar otro comando.

Cuando uso los comandos y subcomandos de racadm, recibo mensajes de error que no entiendo.

Es posible que reciba uno o más de los siguientes errores cuando use los comandos y subcomandos de RACADM:

- Mensajes de errores locales de RACADM: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de errores remotosde RACADM: problemas tales como una dirección IP, nombre de usuario o contraseña incorrectos.

Cuando ejecuto el comando ping con la dirección IP del iDRAC6 desde mi sistema y luego cambio mi tarjeta iDRAC6 entre los modos Dedicado y Compartido durante la respuesta del comando ping, no recibo respuesta.

Borre la tabla ARP en el sistema.

Configuración de múltiples controladoras iDRAC6

Por medio de RACADM, usted puede configurar uno o más iDRAC6 con propiedades idénticas. Cuando realiza una consulta en una controladora iDRAC6 especifica con las identificaciones de grupo y de objeto de la tarjeta, RACADM crea el archivo de configuración **racadm.cfg** a partir de la información obtenida. Si exporta el archivo a una o más tarjetas iDRAC6, podrá configurar los controladores con propiedades idénticas en un periodo mínimo.

NOTA: Algunos archivos de configuración contienen información exclusiva del iDRAC6 (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros iDRAC6.

Para configurar múltiples controladoras iDRAC6, realice los siguientes procedimientos:

1. Utilice RACADM para consultar el iDRAC6 de destino que contiene la configuración adecuada.

   NOTA: El archivo **.cfg** generado no contiene contraseñas de usuario.

   Abra una petición de comandos y escriba:

   ```
   racadm getconfig -f miarchivo.cfg
   ```

   NOTA: La redirección de la configuración de iDRAC6 hacia un archivo por medio de **getconfig -f** sólo se admite con las interfaces local y remota de RACADM.

2. Modifique el archivo de configuración con un editor de textos simple (opcional).

3. Utilice el nuevo archivo de configuración para modificar un iDRAC6 de destino.

   En la petición de comandos, escriba:

   ```
   racadm config -f myfile.cfg
   ```

4. Restablezca el iDRAC6 de destino que fue configurado.

   En la petición de comandos, escriba:

   ```
   racadm racreset
   ```

El subcomando **getconfig -f racadm.cfg** solicita la configuración del iDRAC6 y genera el archivo **racadm.cfg**. Si se requiere, puede configurar el archivo con otro nombre.

Puede usar el comando **getconfig** para ejecutar las siguientes acciones:

- Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice)
- Mostrar todas las propiedades de configuración de usuario por nombre de usuario

El subcomando **config** carga la información en otras tarjetas 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 la petición de comandos:

```
racadm getconfig -f miarchivo.cfg
```

PRECAUCIÓN: Se recomienda que edite este archivo con un editor de textos simple. La utilidad RACADM utiliza un analizador de textos ASCII. Los elementos de formato confunden al analizador y esto puede dañar la base de datos de RACADM.

Creación de un archivo de configuración de iDRAC6

El archivo de configuración del iDRAC6 **<***nombre_de_archivo***>.cfg** se utiliza con el comando `racadm config -f <nombre_de_archivo>.cfg`. Puede usar el archivo de configuración para crear un archivo de configuración (parecido a un archivo **.ini**) y configurar el iDRAC6 a partir de este archivo. Usted puede usar cualquier nombre de archivo y el archivo no requiere una extensión **.cfg** (aunque en este apartado nos refiramos al mismo con dicha extensión).

El archivo **.cfg** se puede:

- Crear
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg`
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y después modificarse

NOTA: Consulte "getconfig" para obtener información sobre el comando **getconfig**.

El archivo **.cfg** se analiza primero para verificar que los nombres de grupo y de objeto sean válidos y que se sigan algunas reglas simples de sintaxis. Los errores se señalan con el número de la línea en la que se detectó el error y un mensaje simple explica el problema. El archivo completo se analiza para confirmar que sea correcto y se muestran todos los errores. Los comandos de escritura no se transmiten al iDRAC6 si se encuentra un error en el archivo **.cfg**. El usuario debe corregir *todos* los errores antes de que pueda realizar cualquier configuración. La opción **-c** se puede usar en el subcomando **config**, que verifica sólo la sintaxis y no realiza operaciones de escritura en el iDRAC6.

Utilice las siguientes directrices al crear un archivo **.cfg**:

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

  El analizador lee en todos los índices de iDRAC6 para ese grupo. Los objetos dentro de dicho grupo son modificaciones simples cuando se configura el iDRAC6. Si un objeto modificado representa un índice nuevo, el índice se crea en el iDRAC6 durante la configuración.

- No se puede especificar el índice que se desea en un archivo **.cfg**.

  Los índices se pueden crear y eliminar, por lo que con el tiempo el grupo se puede fragmentar con índices usados y no usados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método permite tener flexibilidad al momento de agregar anotaciones indexadas en las que usted no necesita hacer coincidencias exactas de índice entre todos los RAC que se administran. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo **.cfg** que se analiza y se ejecuta correctamente en un iDRAC6 no funcione correctamente en otro si todos los índices están llenos y se tiene que agregar un nuevo usuario.

- Utilice el subcomando **racresetcfg** para configurar todas las tarjetas iDRAC6 con propiedades idénticas.

  Use el subcomando **racresetcfg** para restablecer el iDRAC6 a los valores predeterminados originales y luego ejecute el comando `racadm config -f <nombre_de_archivo>.cfg` **.** Asegúrese que el archivo **.cfg** tenga todos los objetos, usuarios, índices y demás parámetros requeridos.

PRECAUCIÓN: Use el subcomando racresetcfg para restablecer la base de datos y la configuración del NIC del iDRAC6 a los valores predeterminados originales y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas del análisis

- Todas las líneas que comienzan con '#' son tratadas como comentarios.

  Una línea de comentario *debe* comenzar en la columna uno. Un carácter "#" en cualquier otra columna se trata como un carácter "#".

  Algunos parámetros de módem pueden incluir caracteres # en la cadena. No se requiere un carácter de escape. Es posible que desee generar un archivo **.cfg** a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y luego realizar un comando `racadm config -f <nombre_de_archivo>.cfg` para un iDRAC6 diferente, sin agregar caracteres de escape.

  Ejemplo:

  ```
  #

  # This is a comment

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # not a comment>

  (#

  # Esto es un comentario

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<# de inicio de módem, no es un comentario>)
  ```

- Todas las anotaciones de grupo deben estar rodeadas por los caracteres "**[**"y "**]**".

  El carácter "**[**" de inicio que denota un nombre de grupo *debe* comenzar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en "Definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6.".

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

  Ejemplo:

  ```
  [cfgLanNetworking] -{nombre de grupo}

  cfgNicIpAddress=143.154.133.121 {nombre de objeto}
  ```

- Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor.

  Se ignorarán los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de una cadena de valores se mantienen sin modificación. Los caracteres a la derecha del símbolo "=" se tomarán tal cual (por ejemplo, un segundo "=" o un símbolo "#", "[", "]", etc.) Todos estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

  Consulte el ejemplo en el punto anterior.

- El analizador de **.cfg** ignora una anotación de objeto de índice.

  El usuario *no puede* especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva anotación en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <nombre del archivo>.cfg` coloca un comentario delante de los objetos de índice, lo que permite al usuario ver los comentarios incluidos.

NOTA: Usted puede crear un grupo indexado manualmente, con el siguiente comando:
`racadm config -g <nombre_de_grupo> -o <objeto anclado> -i <indice 1-16> <nombre de ancla exclusivo>`

- La línea de un grupo indexado *no se puede* eliminar de un archivo **.cfg**.

  El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

  ```
  racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> -i <indice de 1 a 16> ""
  ```

NOTA: Una cadena NULA (que se identifica por dos caracteres "") indica al iDRAC6 que elimine el índice del grupo especificado.

Para ver el contenido de un grupo indexado, use el siguiente comando:

```
racadm getconfig -g <nombre_de_grupo> -i <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]

cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
```

Si escribe `racadm getconfig -f <mi_ejemplo>.cfg`, el comando genera un archivo .cfg para la configuración actual del iDRAC6. Este archivo de configuración se puede usar como ejemplo y como punto de partida para su archivo **.cfg** exclusivo.

Modificación de la dirección IP del iDRAC6

Al modificar la dirección IP del iDRAC6 en el archivo de configuración, elimine todas las anotaciones innecesarias de **<***variable***>**=**valor**. Sólo permanece la etiqueta del grupo variable real con "[" y "]", incluso las dos anotaciones de **<***variable***>**=**valor** que pertenecen al cambio de dirección IP.

Por ejemplo:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1

(#

# Grupo de objeto "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1)
```

Este archivo será actualizado de la siguiente manera:

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

cfgNicGateway=10.35.9.1

(#

# 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 mi_archivo.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 disponibles de red, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Para utilizar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** y active esta función:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

Los comandos brindan la misma funcionalidad de configuración que la utilería de configuración iDRAC6 al momento de inicio cuando se pide que presione <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, consulte Configuración de su sistema para usar iDRAC6.

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de red LAN deseadas.

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN de iDRAC6 se desactivará aun cuando DHCP esté activado.

Modos de iDRAC6

El iDRAC6 puede configurarse en uno de cuatro modos:

- Dedicado
- Compartido
- Compartido con protección de fallos en LOM2
- Compartido con protección de fallos en todos los LOM

La Tabla 5-16 ofrece una descripción de cada modo.

Tabla 5-16. Configuraciones del NIC de iDRAC6

Modo	Descripción
Dedicado	El iDRAC6 utiliza su propia tarjeta de interfaz de red (conector RJ-45) y la dirección MAC del iDRAC para el tráfico de red.
Compartido	El iDRAC6 usa LOM1 en la placa madre.
Compartido con protección de fallos en LOM2	El iDRAC6 utiliza LOM1 y LOM2 como equipo para protección contra fallas. El equipo utiliza la dirección MAC del iDRAC6.
Compartido con protección de fallos en todos los 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

Al acceder a la interfaz por web del iDRAC6, recibo una advertencia de seguridad informando que el nombre del host del certificado SSL no coincide con

el nombre de host del iDRAC6.

El iDRAC6 incluye un certificado de servidor del iDRAC6 predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Cuando se usa este certificado, el explorador de 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 de iDRAC6 emitido para la dirección IP o el nombre de iDRAC del iDRAC6. Cuando se genere la solicitud de firma del certificado (CSR, por sus siglas en inglés) que se usará para emitir el certificado, asegúrese de que el nombre común (CN, por sus siglas en inglés) del CSR concuerde con la dirección IP) (**si el certificado se emite para la IP**) del iDRAC6 (por ejemplo, 192.168.0.120) o el nombre DNS registrado de iDRAC6 (**si el certificado se emite al nombre registrado de iDRAC**).

Para asegurarse de que la CSR coincida con el nombre DNS registrado del iDRAC6:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Red**.
3. En la tabla **Valores comunes**:
    a. Seleccione la casilla de verificación **Registrar el iDRAC en DNS**.
    b. En el campo **Nombre DNS del iDRAC**, introduzca el nombre del iDRAC6.
4. Haga clic en **Aplicar cambios**.

Consulte "Cómo asegurar las comunicaciones de iDRAC6 por medio de certificados SSL y digitales" para obtener más información sobre cómo producir CSR y cómo emitir certificados.

¿Por qué no están disponibles RACADM remota y los servicios basados en web después de un cambio de propiedad?

Es posible que los servicios de RACADM remota y la interfaz basada en web tarden un poco en estar disponibles después de restablecer el servidor web del iDRAC6.

El servidor de web del iDRAC6 se restablece después de los siguientes acontecimientos:

- Cuando la configuración de red o las propiedades de seguridad de la red se cambian mediante la interfaz web de usuario del iDRAC6
- Cuando la propiedad **cfgRacTuneHttpsPort** cambia (incluso cuando un comando config -f <*archivo_de_config*> la cambia)
- Cuando se utiliza **racresetcfg**
- Cuando el iDRAC6 se restablece
- Cuando se carga un nuevo sertificado de servidor SSL

¿Por qué mi servidor DNS no registra mi iDRAC6?

Algunos de los servidores DNS sólo registran nombres de 31 caracteres o menos.

Al acceder a la interfaz web del iDRAC6, recibo una advertencia de seguridad informando que el certificado SSL fue emitido por una autoridad de certificados (CA) que no es confiable.

El iDRAC6 incluye un certificado de servidor del iDRAC6 predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Este certificado no fue emitido por una CA confiable. Para resolver este asunto de seguridad, cargue un certificado de servidor de iDRAC6 que haya sido publicado por una CA confiable (por ejemplo, Microsoft Certificate Authority, Thawte o Verisign). Consulte "Cómo asegurar las comunicaciones de iDRAC6 por medio de certificados SSL y digitales" para obtener más información acerca de la emisión de certificados.

Regresar a la página de contenido

Regresar a la página de contenido

Cómo agregar y configurar usuarios del iDRAC6

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

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 a los usuarios de 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 los usuarios de iDRAC6, realice los pasos a continuación:

NOTA: Debe tener permiso para **Configurar Usuarios** para cambiar un usuario de iDRAC.

1. Haga clic en **Acceso Remoto**→ **Configuración**→ **Usuarios**.

   La página de los Usuarios muestra la siguiente información para los usuarios iDRAC: **ID de usuario, Estado (Activado/Desactivado), Nombre del usuario, Privilegios RAC**, **Privilegios LAN de IPMI**, **Privilegio serial de IPMI**, y estado del **serial sobre LAN (Activado/Desactivado)**. Tabla describe los estados y permisos del usuario para configurar usuarios de iDRAC.

   NOTA: El usuario 1 está reservado para el usuario anónimo de IPMI y no se puede configurar.

2. En la columna **Id. de usuario**, haga clic en un número de identificación de usuario.

   En la página del **Menu Principal del usuario**, puede configurar un usuario, ver un certificado de usuario, cargar un certificado de confianza de una Autoridad de Certificación (CA) o ver un certificado de confianza de una CA.

   Si selecciona **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página de **Configuración de usuario**. Pase al paso 4.

   Si selecciona una opción en **Configuración de tarjeta inteligente**, vea Tabla .

3. En la página de **Configuración de usuario**, configure lo siguiente:
   - El nombre de usuario, contraseña, y los permisos de acceso para un usuario nuevo o existente de iDRAC. Tabla describe **Configuración global de usuario**.
   - Los privilegios IPMI del usuario. La Tabla 6-4 describe los **Privilegios de usuario de IPMI** necesarios para configurar los privilegios de LAN del usuario.
   - Los privilegios de usuario de iDRAC. Tabla 6-5 describe los **Privilegios de usuario de iDRAC**.
   - Permisos de acceso de Grupo de iDRAC. describe los Tabla 6-6**Permisos de Grupo de iDRAC**.

4. Cuando termina, haga clic en **Aplicar cambios**.

5. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 6-7.

Tabla 6-1. Estados y Permisos de usuario

Valor	Descripción
Identificación de usuario	Muestra la lista secuencial de los números ID de usuarios. Cada campo en **ID de usuario** contiene uno de los 16 números de ID de usuario predefinidos. Este campo no se puede editar.
Estado	Muestra el estado de inicio de sesión del usuario: Activado o Desactivado. (Desactivado es elpredeterminado). **NOTA:** El usuario 2 está activado por defecto.
Nombre de usuario	Muestra el nombre de sesión del usuario. Especifica un nombre de usuario de iDRAC de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único.

	NOTA: Los nombres de usuario de iDRAC no pueden incluir los caracteres **/** (diagonal) ni **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Privilegio RAC	Muestra el grupo (nivel de privilegio) al que está asignado el usuario (Adminstrador, Operador, Solo lectura o Ninguno).
Privilegio LAN de IPMI	Muestra el nivel de privilegio LAN de IPMI al que está asignado el usuario (Adminstrador, Operador, Solo lectura o Ninguno).
Privilegio Serial de IPMI	Muestra el nivel de privilegio del Puerto Serial de IPMI al que está asignado el usuario (Adminstrador, Operador, Solo lectura o Ninguno).
Comunicación en serie en la LAN	Permite o revoca el permiso al usuario usar la comunicación en serie en la LAN de IPMI.

Tabla 6-2. Opciones de configuración de la tarjeta inteligente

Opción	Descripción
Ver **certificado de usuario**	Muestra la página de certificado de usuario que se cargó en el iDRAC.
Cargar **certificado de CA de confianza**	Permite cargar el certificado de CA de confianza en el iDRAC e importarlo al perfil del usuario.
Ver certificado de CA de confianza	Muestra el certificado de CA de confianza que se cargó en el iDRAC. El certificado de CA de confianza lo emite la CA que está autorizada para emitir certificados para usuarios.

Tabla 6-3. Configuración general de usuarios

Identificación de usuario	Uno de los 16 números preconfigurados de identificación de usuario.
Activar el usuario	Cuando está seleccionado, indica que el acceso del usuario al iDRAC6 está activado. Cuando no está seleccionado, el acceso de usuario está desactivado.
Nombre de usuario	Un nombre de usuario de hasta 16 caracteres.
Cambiar contraseña	Activa los campos **Nueva contraseña** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán.
Confirmar nueva contraseña	Vuelva a escribir la contraseña del usuario del iDRAC para confirmarla.

Tabla 6-4. Privilegios del usuario de IPMI

Propiedad	Descripción
Privilegio máximo permitido de usuario de LAN	Especifica el privilegio máximo del usuario en el canal de LAN de IPMI para uno de los siguientes grupos de usuarios: **Administrador**, **Operador**, **Usuario** o **Ninguno**.
Privilegio máximo permitido de usuario de puerto serie	Especifica el privilegio máximo del usuario en el canal Serial 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
Roles	Especifica el privilegio máximo de usuario de iDRAC del usuario a uno de los siguientes: **Administrador**, **Operador**, **Solo lectura** o **Ninguno**. Consulte Tabla 6-6 para ver los **Permisos del Grupo de iDRAC**.
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC.
Configurar iDRAC	Permite al usuario configurar el iDRAC.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros de iDRAC.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de Control del Servidor.
Acceder a redirección de consola	Activa la capacidad del usuario de ejecutar redirección de consola.
Acceder a los medios virtuales	Activa la capacidad del usuario de ejecutar y usar los medios virtuales.
Probar alertas	Activa la capacidad del usuario de enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Activa la capacidad del usuario de ejecutar comandos de diagnóstico.

Tabla 6-6. Permisos de grupo del iDRAC

Grupo de usuarios	Permisos concedidos
Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.
Operador:	Selecciona cualquier combinación de los permisos siguientes: **Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de acción del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**
Sólo lectura	**Inicio de sesión en iDRAC**
Ninguno	Sin permisos asignados

Tabla 6-7. Botones de la página de configuración de usuario

Botón	Acción
Imprimir	Imprime los valores de la **Configuración de usuario** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Configuración de usuario**.
Volver a la página de usuarios	Regresa a la **página de usuarios**.
Aplicar cambios	Guarda todos los nuevos valores que se hayan introducido en la configuración de usuario.

Uso de la utilidad RACADM para configurar usuarios del iDRAC6

NOTA: Se debe haber iniciado sesión como usuario **root** para ejecutar los comandos de RACADM en un sistema remoto con Linux.

La interfaz web de iDRAC6 es la forma más rápida para configurar un usuario iDRAC6. Si prefiere configuración mediante línea de comandos o secuencias de comandos o si necesita configurar varias tarjetas iDRAC6, utilice RACADM, que se instala con los agentes de iDRAC6 en el sistema administrado.

Para configurar varias tarjetas iDRAC6 con valores de configuración idénticos, realice uno de los siguientes procedimientos:

- Use los ejemplos de RACADM en esta sección como guía para crear un archivo de procesamiento en lote de comandos RACADM y después ejecute el archivo de procesamiento en lote en cada sistema administrado.
- Cree un archivo de configuración de iDRAC6 según se describe en "Generalidades del subcomando RACADM" y ejecute el subcomando **racadm config** en cada sistema administrado por medio del mismo archivo de configuración.

Antes de comenzar

Puede configurar hasta 16 usuarios en la base de datos de propiedades del iDRAC6. Antes de activar manualmente a un usuario del iDRAC6, verifique si existe algún usuario actual. Si está configurando un iDRAC6 nuevo o si ha ejecutado el comando **racadm racresetcfg**, el único usuario actual es root con la contraseña `calvin`. El subcomando **racresetcfg** restablece los valores predeterminados originales del DRAC6.

PRECAUCIÓN: Tenga cuidado cuando utilice el comando racresetcfg, pues con éste se restablecen los valores predeterminados de *todos* los parámetros de configuración. Todos los cambios anteriores se perderán.

NOTA: Los usuarios se pueden activar o desactivar posteriormente. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC6.

Para verificar si existe un usuario, escriba el comando siguiente en la petición de comandos:

```
racadm getconfig -u <nombre_de_usuario>
```

O bien:

escriba el comando siguiente una vez para cada índice de 1 a 16:

```
racadm getconfig -g cfgUserAdmin -i <índice>
```

NOTA: También puede escribir racadm getconfig -f <mi_archivo.cfg> y ver o editar el archivo **mi_archivo.cfg**, que incluye todos los parámetros de configuración del iDRAC6.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

Si el objeto **cfgUserAdminUserName** no tiene un valor, el número de índice que indica el objeto **cfgUserAdminIndex** está disponible para su uso. Si hay un nombre después del signo "=", el nombre de usuario tomará ese índice.

NOTA: Cuando agrega o borra un usuario manualmente con el subcomando **racadm config**, *debe especificar* el índice con la opción **-i**. Note que el objeto **cfgUserAdminIndex** mostrado en el ejemplo anterior contiene un carácter '#'. Asimismo, si utiliza el comando **racadm config** -**f racadm.cfg** para

especificar el número de grupos/objetos a 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 tarjetas iDRAC6 con los mismos valores.

Adición de un usuario iDRAC6

Para agregar un nuevo usuario a la configuración del RAC, se pueden usar unos cuantos comandos básicos. En general, realice los siguientes procedimientos:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los siguientes privilegios del usuario:
   - Privilegio iDRAC
   - Privilegio LAN de IPMI
   - Privilegio Serial de IPMI
   - Privilegio de comunicación serial en LAN
4. Active el usuario.

Ejemplo

El siguiente ejemplo describe cómo agregar un nuevo usuario de nombre "Juan" con la contraseña "123456" y privilegios de inicio de sesión en el RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Para verificarlo, use uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig –g cfgUserAdmin –i 2
```

Eliminación de un usuario iDRAC6

Al usar RACADM, los usuarios se deben desactivar manual e individualmente. Los usuarios no se pueden eliminar por medio de un archivo de configuración.

El ejemplo siguiente ilustra la sintaxis de comando que se puede usar para eliminar un usuario de RAC:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <índice> ""
```

Una cadena nula de dos caracteres de comillas ("") indica al iDRAC6 que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.

Activación de un usuario del iDRAC6 con permisos

Para activar un usuario con permisos administrativos específicos (autoridad en base a funciones), encuentre primero un índice de usuario disponible por medio de los pasos de la sección "Antes de comenzar". Posteriormente, escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña.

NOTA: Consulte la Tabla B-2 para ver una lista de los valores válidos de máscara de bits para los privilegios de usuario específicos. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios habilitados.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <índice> <valor de máscara de bits de privilegios de usuario>
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de iDRAC6 con Microsoft Active Directory

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Un servicio de directorio se usa para mantener una base de datos común de toda la información necesaria para controlar a usuarios, equipos, impresoras, etc., en una red. Si la empresa usa el software de servicio Microsoft® Active Directory®, puede configurarlo de manera que tenga acceso al iDRAC6, lo que le permite agregar privilegios de usuario de iDRAC6 a los usuarios existentes y controlar estos privilegios en el software Active Directory.

NOTA: El uso de Active Directory para reconocer usuarios del iDRAC6 se admite en los sistemas operativos Microsoft Windows® 2000, Windows Server® 2003 y Windows Server 2008.

La tabla 7-1 muestra los nueve privilegios de usuario de Active Directory del iDRAC6.

Tabla 7-1. Privilegios de usuario del iDRAC6

Privilegio	Descripción
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC6.
Configurar iDRAC	Permite al usuario configurar el iDRAC6.
Configurar usuarios	Permite al usuario otorgar acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros de iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a redirección de consola	Permite al usuario ejecutar la redirección de consola.
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Requisitos previos para activar la autentificación de Active Directory para el 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 necesitará activar la Capa de conexión segura (SSL) en todos los controladores de dominio a los que se conecte el iDRAC6. Consulte "Activación de SSL en un controlador de dominio" para obtener información más específica.

Mecanismos de autenticación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: mediante la solución de *esquema ampliado*, que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell. O puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las secciones siguientes para obtener más información sobre estas soluciones.

Cuando se usa Active Directory para configurar el acceso al iDRAC6, se debe elegir la solución de esquema ampliado o de esquema estándar.

Las ventajas de usar la solución de esquema ampliado son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Se brinda máxima flexibilidad para configurar el acceso de los usuarios en diferentes tarjetas del iDRAC6 con distintos niveles de privilegios.

La ventaja de utilizar la solución de esquema estándar radica en que no se requiere una ampliación del esquema, ya que la configuración predeterminada del esquema de Active Directory que brinda Microsoft proporciona todas las clases de objetos necesarias.

Generalidades del esquema ampliado de Active Directory

Para utilizar la solución de esquema ampliado, es necesaria una ampliación de esquema de Active Directory según se describe en la siguiente sección.

Extensión del esquema de Active Directory

Importante: la ampliación del esquema para este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Deberá ampliar el nuevo esquema e instalar el nuevo complemento Microsoft Management Console (MMC) de usuarios y equipos de Active Directory en su directorio. El esquema anterior no funciona con este producto.

NOTA: La ampliación del nuevo esquema y la instalación de la nueva ampliación en el complemento de usuarios y equipos de Active Directory no afectan los productos anteriores.

Puede encontrar el complemento MMC de usuarios y equipos de Active Directory y la ampliación de esquema en el DVD *Dell Systems Management Tools and Documentation*. Para obtener más información, consulte "Extensión del esquema de Active Directory" e "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory". Para obtener más detalles sobre la ampliación del esquema para iDRAC6 y la instalación del complemento MMC de usuarios y equipos de Active Directory, consulte la *Guía del usuario de instalación y seguridad de Dell OpenManage* en **support.dell.com\manuals**.

NOTA: Cuando crea objetos de asociación o de dispositivo del iDRAC, asegúrese de seleccionar **Dell Remote Management Object Advanced**.

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden ampliar la base de datos de Active Directory al agregar sus propios atributos y clases únicos para solucionar necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que es se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de Identificadores de Objeto de Active Directory (OID) de modo que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para ampliar el esquema en Microsoft Active Directory, Dell recibió OID exclusivos, extensiones de nombre exclusivas e identificaciones de atributo vinculadas exclusivamente para las clases y los atributos agregados al servicio de directorio.

La extensión de Dell es: dell

El OID base de Dell es: 1.2.840.113556.1.8000.1280

El rango del LinkID de RAC es: 12070 a 12079

Descripción de las extensiones de esquema del iDRAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha ampliado el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o los grupos que tienen un conjunto específico de privilegios para uno o varios dispositivos del iDRAC. Este modelo proporciona máxima flexibilidad al Administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC y dispositivos del iDRAC en la red sin aumentar demasiado la complejidad.

Descripción general de los objetos de Active Directory

Para cada uno de los iDRAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de iDRAC. Puede crear varios objetos de asociación, y cada objeto de asociación puede vincularse a cuantos usuarios, grupos de usuarios u objetos de dispositivo del iDRAC sean necesarios. Los usuarios y los grupos de usuarios del iDRAC pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación puede vincularse (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo del iDRAC) sólo a un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los iDRAC específicos.

El objeto del 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 autenticar.

La Figura 7-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

Ilustración 7-1. Configuración típica de los objetos de Active Directory

Usted puede crear tantos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de

dispositivo del iDRAC por cada iDRAC de la red que desea integrar con Active Directory para autentificación y autorización con iDRAC.

El objeto de asociación permite toda cantidad de usuarios o grupos, así como de objetos de dispositivo del iDRAC. Sin embargo, el objeto de asociación sólo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los *usuarios* con *privilegios* en los iDRAC.

La extensión de Dell al complemento MMC de usuarios y equipos de Active Directory sólo permite asociar el objeto de privilegio y los objetos del iDRAC del mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC de otro dominio se agregue como miembro del producto del objeto de asociación.

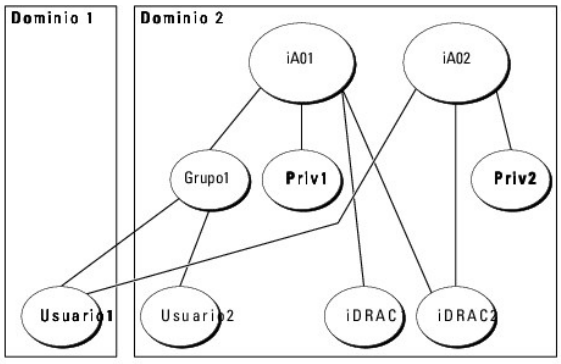
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema ampliado admiten todo tipo de grupos de usuarios o todo grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema ampliado

El mecanismo de autenticación del esquema ampliado admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados con el mismo usuario entre distintos objetos de asociación. En otras palabras, la autenticación del esquema ampliado acumula privilegios para permitir al usuario el súper conjunto de todos los privilegios asignados que corresponden a los distintos objetos de privilegio asociados al mismo usuario.

La Figura 7-2 muestra un ejemplo de la acumulación de privilegios por medio del esquema ampliado.

Ilustración 7-2. Acumulación de privilegios para un usuario



La figura muestra dos objetos de asociación: OA1 y OA2. 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 iDRAC2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; y Priv2 tiene los privilegios: Inicio de sesión en iDRAC, Configurar el iDRAC y Probar alertas. Como resultado, el Usuario1 tiene ahora el conjunto de privilegios: Inicio de sesión en iDRAC, Medios virtuales, Borrar registros, Configurar el iDRAC y Probar alertas, que es el conjunto de privilegios combinados de Priv1 y Priv2.

La autentificación del esquema ampliado acumula privilegios para permitir que el usuario tenga el conjunto máximo de privilegios según los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

En esta configuración, el Usuario1 tiene privilegios de Priv1 y Priv2 en iDRAC2. El Usuario1 tiene privilegios de Priv1 en iDRAC1 solamente. El Usuario2 tiene privilegios de Priv1 tanto en iDRAC1 como en iDRAC2. Además, esta ilustración muestra que el Usuario1 puede estar en un dominio diferente y ser miembro de un grupo anidado.

Configuración de Active Directory de esquema ampliado para acceder al iDRAC

Antes de usar Active Directory para acceder al iDRAC6, debe configurar el software Active Directory y el iDRAC6 llevando a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (consulte "Extensión del esquema de Active Directory").
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory").
3. Agregue usuarios del iDRAC6 y sus privilegios a Active Directory (consulte "Cómo agregar usuarios y privilegios de iDRAC a Active Directory").
4. Active SSL en cada uno de los controladores de dominio (consulte "Activación de SSL en un controlador de dominio").
5. Configure las propiedades de Active Directory del iDRAC6 por medio de la interfaz web del iDRAC6 o RACADM (consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema ampliado por medio de RACADM").

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

Puede ampliar el esquema por medio de uno de los métodos siguientes:

- Utilidad Dell Schema Extender

- Archivo de secuencia de comandos LDIF

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation*, en los siguientes directorios respectivamente:

- *Unidad de DVD*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <**Unidad de DVD >:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Para usar los archivos LDIF, consulte las instrucciones en el archivo readme (léame) que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, consulte "Uso del ampliador de esquema de Dell".

Puede copiar y ejecutar el ampliador de esquema o los archivos LDIF desde cualquier ubicación.

Uso del ampliador de esquema de Dell

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 el ampliador de esquema de Dell.
5. Haga clic en **Finish** (Finalizar).

   El esquema ha sido extendido. Para verificar la ampliación del esquema, utilice el complemento de esquema de Active Directory y MMC para controlar que existan los siguientes elementos:

   - Clases (consulte de la Tabla 7-2 a la Tabla 7-7)
   - Atributos (Tabla 7-8)

Consulte la documentación de Microsoft para obtener información acerca de cómo utilizar el complemento de esquema de Active Directory y MMC.

Tabla 7-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 7-3. Clase dellRacDevice

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
Descripción	Representa el dispositivo iDRAC de Dell. El dispositivo iDRAC debe estar configurado como dellRacDevice en Active Directory. Esta configuración hace posible que el iDRAC envíe consultas de Protocolo de acceso ligero de directorio (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	**dellSchemaVersion** **dellRacType**

Tabla 7-4. Clase delliDRACAssociationObject

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo

Atributos	**dellProductMembers** **dellPrivilegeMember**

Tabla 7-5. Clase dellRAC4Privileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Descripción	Se usa para definir los privilegios (derechos de autorización) del dispositivo iDRAC.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabla 7-6. Clase dellPrivileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	**dellRAC4Privileges**

Tabla 7-7. Clas dellProduct

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	**dellAssociationMembers**

Tabla 7-8. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/Descripción	**OID asignado/ Identificador de objeto de sintaxis**	**Con un solo valor**
dellPrivilegeMember Lista de los objetos de dellPrivilege Dell que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este 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 distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE

TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellIsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de redirección de consola en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena en que se ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el enlace de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory

Cuando se amplía el esquema en Active Directory, también debe ampliarse el complemento de usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC, los usuarios y los grupos de usuarios, y las asociaciones y privilegios del iDRAC.

Cuando instala el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation*, puede ampliar el complemento si selecciona la opción **Complemento de usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener más instrucciones sobre la instalación del software de administración de sistemas. Para sistemas operativos Windows de 64 bits, el instalador del complemento se ubica en **<unidad de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**.

Para obtener más información acerca del complemento de usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Instalación de Administrator Pack

Debe instalar el paquete de administrador en cada sistema que administre los objetos de iDRAC de Active Directory. Si no instala el paquete de administrador, no podrá ver el objeto iDRAC de Dell en el contenedor.

Para obtener más información, consulte "Cómo abrir el complemento de usuarios y equipos de Active Directory".

Cómo abrir el complemento de usuarios y equipos de Active Directory

Cómo abrir el complemento de usuarios y equipos de Active Directory:

1. Si está conectado en el controlador del dominio, haga clic en **Inicio Herramientas administrativas→ Usuarios y equipos de Active Directory.** .

   Si no está conectado en el controlador de dominio, debe tener el Administrator Pack de Microsoft correspondiente instalado en el sistema local. Para instalar este Administrator Pack, haga clic en **Inicio→ Ejecutar**, escriba `MMC` y oprima **Entrar**.

   Aparece MMC.

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).
3. Haga clic en **Agregar o quitar complemento**.
4. Seleccione el **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar.**
5. Haga clic en **Cerrar** y haga clic en **Aceptar**.

Cómo agregar usuarios y privilegios de iDRAC a Active Directory

El complemento de usuarios y equipos de Active Directory ampliado por Dell permite agregar usuarios y privilegios del iDRAC mediante la creación de objetos de asociación y de privilegio del iDRAC. Para agregar cada tipo de objeto, realice los pasos a continuación:

- Cree un objeto de dispositivo del iDRAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Configuración de un objeto de asociación

Creación de un objeto de dispositivo del iDRAC

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Aparece la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC que usted va a introducir en el Paso A de "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6".
4. Seleccione **Objeto de dispositivo de iDRAC**.
5. Haga clic en **OK** (Aceptar).

Creación de un objeto de privilegio

NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Aparece 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 lengüeta **Privilegios de administración remota** y seleccione los privilegios que desea otorgar al usuario.

Creación de un objeto de asociación

NOTA: El objeto de asociación del iDRAC se deriva de un grupo y su alcance está establecido en Local de dominio.

1. En la ventana **Raíz de 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. Seleccione el ámbito para el **objeto de asociación**.
6. 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 del iDRAC.

Puede agregar grupos de usuarios. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

1. Haga clic con el botón derecho del mouse en el **objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de grupo de usuarios o usuario y haga clic en **Aceptar**.

Haga clic en la lengüeta **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentifican en un dispositivo iDRAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

1. Seleccione la ficha **Objetos de privilegio** y haga clic en **Agregar**.
2. Escriba el nombre del objeto de privilegio y haga clic en **Aceptar**.

Haga clic en la lengüeta **Productos** para agregar un dispositivo iDRAC conectado a la red disponible para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de iDRAC a un objeto de asociación.

Cómo agregar dispositivos de iDRAC

Para agregar dispositivos de iDRAC:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Ingrese el nombre del dispositivo iDRAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz basada en web del iDRAC6.
3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
4. Haga clic en la ficha **Configuración** y seleccione **Active Directory**.
5. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparece la página **Paso 1 de 4 Configuración y administración de Active Directory**.
6. En **Configuración de certificados**, marque **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9.

7. En **Cargar un certificado de CA de Active Directory**, ingrese la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado.

NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

8. Haga clic en **Cargar**.

   Aparece la información del certificado de CA de Active Directory que cargó.

9. Haga clic en **Siguiente** para ir al **Paso 2 de 4** de **Configuración y administración de Active Directory**.

10. Haga clic en **Activar Active Directory**.

11. Haga clic en **Agregar** para ingresar el nombre de dominio de usuario.

12. Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**. Tenga en cuenta que este paso es opcional. Si configura una lista de dominios de usuario, la lista estará disponible en la pantalla de inicio de sesión de la interfaz basada en web. Usted puede elegir de la lista y luego sólo debe ingresar el nombre de usuario.

13. Ingrese el **Tiempo de espera** en segundos para especificar el tiempo que iDRAC6 tendrá que esperar para las respuestas de Active Directory. El valor predeterminado es 120 segundos.

14. Ingrese la Dirección de servidor del controlador de dominio. Puede ingresar hasta tres servidores Active Directory para procesar los inicios de sesión, pero es necesario que configure al menos un servidor. Para hacerlo, ingrese la dirección IP o el nombre de dominio completo (FQDN). iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.

15. Haga clic en **Siguiente** para ir al **Paso 3 de 4** de **Configuración y administración de Active Directory**.

16. En **Selección del esquema**, haga clic en **Esquema ampliado.**

17. Haga clic en **Siguiente** para ir al **Paso 4 de 4** de **Configuración y administración de Active Directory**.

18. En **Configuración del esquema ampliado**, ingrese el nombre del iDRAC y el nombre de dominio para configurar el objeto de dispositivo del iDRAC. El nombre de dominio del iDRAC es el dominio en el que se crea el objeto del iDRAC.

19. Haga clic en **Finalizar** para guardar la configuración del esquema ampliado de Active Directory.

    El servidor web del iDRAC6 lo regresa automáticamente a la página **Configuración y administración de Active Directory**.

20. Haga clic en **Comprobar configuración** para controlar la configuración del esquema ampliado de Active Directory.

21. Ingrese su nombre de usuario y contraseña de Active Directory.

    Visualizará los resultados de la prueba y el registro de la misma. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Vaya a la página **Acceso remoto→ Configuración→ Red** para configurar los servidores DNS en forma manual o use DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema ampliado.

Configuración de Active Directory con esquema ampliado por medio de RACADM

Use los comandos siguientes para configurar el componente Active Directory del iDRAC con el esquema ampliado mediante la CLI de RACADM en vez de la interfaz web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o
   cfgADRacName <nombre común de RAC>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nombre completo del dominio del RAC>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

```
racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>
```

NOTA: Es necesario configurar al menos una de las tres direcciones. iDRAC intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. Cuando selecciona la opción de esquema ampliado, éstas son las direcciones FQDN o IP de los controladores de dominio donde está ubicado el dispositivo iDRAC. Los servidores del catálogo global no se utilizan en el modo de esquema ampliado.

NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.

Si desea desactivar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

En este caso, no tiene que cargar un certificado de CA.

Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, deberá cargar un certificado de CA con el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

racadm sslcertupload -t 0x2 -f <certificado raíz de CA de ADS>
```

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si el DHCP está activado en el iDRAC y usted desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando RACADM:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. Si el DHCP está deshabilitado en el iDRAC o si desea introducir manualmente las direcciones IP de DNS, escriba los siguientes comandos RACADM:

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

   racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
   ```

4. Si desea configurar una lista de dominios de usuario para ingresar el nombre de usuario sólo cuando se inicia sesión en la interfaz basada en web del iDRAC6, escriba el siguiente comando:

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <índice>
   ```

   Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

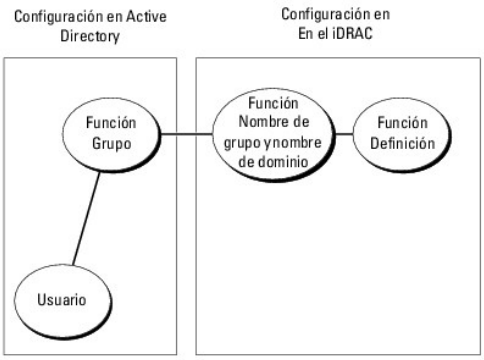
   Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

5. Presione **Entrar** para completar la configuración de Active Directory con esquema ampliado.

Generalidades del esquema estándar de Active Directory

Como se muestra en la Figura 7-3, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en el iDRAC6.

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 ampliado, la función y el nivel de privilegios se definen en cada iDRAC6 y no en Active Directory. Se pueden configurar y definir hasta cinco grupos de funciones en cada iDRAC. Tabla 7-9 muestra los privilegios predeterminados del grupo de funciones.

Tabla 7-9. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel predeterminado de privilegios	Permisos concedidos	Máscara de bits
Grupo de funciones 1	Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**.	0x000001ff
Grupo de funciones 2	Operador:	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC, Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas, Ejecutar comandos de diagnóstico**	0x000000f9
Grupo de funciones 3	Sólo lectura	Inicio de sesión en iDRAC	0x00000001
Grupo de funciones 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de funciones 5	Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios y los grupos de funciones conectados, así como los grupos anidados, están en el mismo dominio, deben configurarse en el iDRAC6 sólo las direcciones de dominio de los controladores. En este caso de dominio único, se admiten todos los tipos de grupos.

Si todos los usuarios y los grupos de funciones conectados, o cualquiera de los grupos anidados, son de múltiples dominios, deben configurarse en el iDRAC6 las direcciones del servidor de Catálogo global. En este caso de dominio múltiple, todos los grupos de función y grupos anidados, si los hubiera, deben ser del tipo Grupo universal.

Configuración de Active Directory de esquema estándar para acceder al iDRAC

Debe realizar los pasos siguientes para configurar Active Directory antes de que los usuarios de Active Directory puedan acceder al iDRAC6:

1. En un servidor de Active Directory (controlador de dominio), abra el **complemento de usuarios y equipos de Active Directory.**
2. Cree un grupo o seleccione un grupo existente. Los nombres del grupo y de este dominio deben configurarse en el iDRAC6 por medio de la interfaz basada en web o por medio de RACADM (consulte "Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6" o "Configuración de Active Directory con esquema estándar vía RACADM").
3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para que pueda tener acceso al iDRAC.

Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz basada en web del iDRAC6.
3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
4. Haga clic en la ficha **Configuración** y seleccione **Active Directory**.
5. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Active Directory**.

   Aparece la página **Paso 1 de 4 Configuración y administración de Active Directory**.
6. En **Configuración de certificados**, marque **Activar validación de certificados** si desea validar el certificado SSL de sus servidores Active Directory; de lo contrario, vaya al paso 9**.**
7. En **Cargar un certificado de CA de Active Directory**, ingrese la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado.

   NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.
8. Haga clic en **Cargar**.

   Aparece la información del certificado de CA de Active Directory que cargó.
9. Haga clic en **Siguiente** para ir al **Paso 2 de 4** de **Configuración y administración de Active Directory**.
10. Haga clic en **Activar Active Directory**.
11. Haga clic en **Agregar** para ingresar el nombre de dominio de usuario.
12. Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**.
13. Ingrese el **Tiempo de espera** en segundos para especificar el tiempo que iDRAC6 tendrá que esperar para las respuestas de Active Directory. El valor predeterminado es 120 segundos.
14. Ingrese la Dirección de servidor del controlador de dominio. Puede ingresar hasta tres servidores Active Directory para procesar los inicios de sesión, pero es necesario que configure al menos un servidor. Para hacerlo, ingrese la dirección IP o el nombre de dominio completo (FQDN). iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.
15. Haga clic en **Siguiente** para ir al **Paso 3 de 4** de **Configuración y administración de Active Directory**.
16. En **Selección del esquema**, haga clic en **Esquema estándar.**
17. Haga clic en **Siguiente** para ir al **Paso 4a de 4** de **Configuración y administración de Active Directory.**
18. En **Configuración de esquema estándar**, ingrese la dirección del servidor del Catálogo global para especificar su ubicación en Active Directory. Debe configurar la ubicación de al menos un servidor del Catálogo global.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.

    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.
19. En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

    Aparece la página del **Paso 4b de 4**.
20. Especifique el **Nombre del grupo de funciones**.

    El **Nombre del grupo de funciones** que identifica el grupo de funciones en Active Directory relacionado con el iDRAC.
21. Especifique el **Dominio del grupo de funciones**, que es el dominio del grupo de funciones.

22. Especifique los **Privilegios del grupo de funciones** seleccionando el **Nivel de privilegio del grupo de funciones**. Por ejemplo, si selecciona **Administrador**, se seleccionan todos los privilegios para dicho nivel de permiso.

23. 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.**

24. Repita los pasos 18 a 22 para configurar más grupos de funciones, o haga clic en **Finalizar** para regresar a la página **Configuración y administración de Active Directory donde se visualizan todas las configuraciones** del esquema **estándar**.

25. Haga clic en **Comprobar configuarción** para controlar la configuración del esquema estándar de Active Directory.

26. Ingrese su nombre de usuario y contraseña de iDRAC6.

    Visualizará los resultados de la prueba y el registro de la misma. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC para admitir el inicio de sesión en Active Directory. Vaya a la página **Acceso remoto→ Configuración→ Red** para configurar los servidores DNS en forma manual o use DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema estándar.

Configuración de Active Directory con esquema estándar vía RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC con esquema estándar por medio de la CLI de RACADM en lugar de hacerlo mediante la interfaz basada en web.

1. Abra una petición de comando y escriba los siguientes comandos de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 2
   ```

   ```
   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupName <nombre común del grupo de funciones>
   ```

   ```
   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupDomain <nombre de dominio completo>
   ```

   ```
   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupPrivilege <Número de máscara de bits para
   permisos de usuarios específicos>
   ```

   NOTA: Para obtener los valores del número de máscara de bits, consulte Tabla B-2.

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.

   NOTA: Ingrese el FQDN del controlador de dominio, *no* solo el FQDN del dominio. Por ejemplo, ingrese `nombredeservidor.dell.com` en vez de `dell.com`.

   NOTA: Es necesario configurar al menos una de las 3 direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   NOTA: El servidor del Catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. En el caso de este dominio múltiple, sólo se puede utilizar el Grupo universal.

   NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio si tiene activada la validación de certificado.

   Si desea desactivar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
   ```

   En este caso, no es necesario cargar ningún certificado de la Autoridad de certificados (CA).

Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <certificado raíz de CA de ADS>
```

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si el DHCP está activado en el iDRAC6 y usted desea usar el DNS proporcionado por el servidor DHCP, escriba los siguientes comandos RACADM:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. Si 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 principal de DNS>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

4. Si desea configurar una lista de dominios de usuario para ingresar el nombre de usuario sólo cuando se inicia sesión en la interfaz basada en 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.

Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

Prueba de las configuraciones realizadas

Si desea verificar si su configuración funciona o si desea diagnosticar el problema en caso de errores al iniciar sesión en Active Directory, puede realizar pruebas de la configuración en la interfaz basada en web de iDRAC6.

Al finalizar la configuración en la interfaz basada en web de iDRAC6, haga clic en **Configuración de prueba** en la parte inferior de la página. Deberá ingresar un nombre de usuario de prueba (por ejemplo, nombredeusuario@dominio.com) y una contraseña para realizarla prueba. Según la configuración, completar todos los pasos de la prueba y mostrar los resultados de cada paso puede tardar un tiempo. Aparecerá un registro detallado de la prueba en la parte inferior de la página de resultados.

Si se produce un error en cualquiera de los pasos, observe la información que aparece en el registro de la prueba para identificar el error y su posible solución. Para obtener información sobre los errores más frecuentes, consulte "Preguntas frecuentes."

Si desea efectuar cambios en la configuración, haga clic en la ficha **Active Directory** y modifique la configuración según las instrucciones detalladas.

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 certificación (CA), cuyo certificado raíz se carga en el iDRAC. En otras palabras, para que el iDRAC pueda autenticarse en *cualquier* controlador de dominio -sin importar si es el controlador de dominio raíz o secundario- el controlador de dominio debe tener un certificado habilitado con SSL firmado por la CA del dominio.

Si va a usar la Entidad emisora de certificados raíz de Microsoft para asignar *automáticamente* todos los controladores de dominio a un certificado SSL, realice los pasos siguientes para activar el SSL en cada controlador de dominio:

1. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio→ Herramientas administrativas→ Política de seguridad del dominio**.
   b. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   c. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado de CA del controlador de dominio raíz a iDRAC

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si está utilizando una CA independiente, los siguientes pasos pueden presentar diferencias.

1. Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **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 o 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 con el botón derecho en el mismo, seleccione **Todas las tareas** y haga clic en **Exportar...**
12. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
15. Cargue el certificado que guardó en el iDRAC en el paso 14.

    Para cargar el certificado por medio de RACADM, consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema estándar vía RACADM."

    Para cargar el certificado por medio de la interfaz basada en la web, consulte "Configuración de Active Directory con esquema ampliado con la interfaz web del iDRAC6" o "Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6."

Cómo importar el 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, deberá cargar también el certificado de servidor del iDRAC en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de cliente durante la fase de inicialización de una sesión SSL.

Use el siguiente procedimiento para importar el certificado SSL de firmware del iDRAC6 a todas las listas de certificados confiables del controlador de dominio.

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si el certificado SSL de firmware del iDRAC6 está firmado por una CA reconocida y dicho certificado ya se encuentra en la lista de Autoridades de certificación de raíz confiables del controlador de dominio, no es necesario realizar los pasos detallados en esta sección.

El certificado SSL de iDRAC es el certificado idéntico que se usa para el Web Server de iDRAC. Todos los controladores del iDRAC se envían con un certificado predeterminado firmado automáticamente.

Para descargar el certificado SSL del iDRAC, ejecute el siguiente comando 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 iDRAC en la lista de **Autoridades de certificación de raíz confiables** de cada controlador de dominio.

   Si ha instalado su propio certificado, asegúrese que la CA que firma su certificado esté en la lista **Autoridad de certificación de raíz confiable**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.

5. Haga clic en **Siguiente** y seleccione si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o desplácese a un almacén de su elección.

6. Haga clic en **Terminar** y luego en **Aceptar**.

Uso de Active Directory para iniciar sesión en el iDRAC6

Puede utilizar Active Directory para iniciar sesión en el iDRAC6 mediante uno de los siguientes métodos:

- Interfaz basada en web
- RACADM remota
- Consola serie o Telnet

La sintaxis de inicio de sesión la misma para los tres métodos:

<nombre_de_usuario@dominio>

O bien:

*<dominio>**<nombre_de_usuario>* o *<dominio>*/*<nombre_de_usuario>*

donde *nombre_de_usuario* es una cadena ASCII de 1 a 256 bytes.

No se permite usar espacios en blanco ni caracteres especiales (como \, / ó @) en el nombre de usuario ni en el nombre de dominio.

NOTA: No se pueden especificar nombres de dominio NetBIOS, como "América", porque estos nombres no se pueden resolver.

Si inicia sesión en la interfaz basada en web y ha configurado dominios de usuario, la página de inicio de sesión de la interfaz basada en web brindará un menú desplegable de todos los dominios de usuario para que seleccione el deseado. Si selecciona un dominio de usuario del menú desplegable, sólo debe ingresar el nombre de usuario. Aun si selecciona **Este iDRAC**, podrá iniciar sesión como usuario de Active Directory si utiliza la sintaxis de inicio de sesión descripta más arriba en "Uso de Active Directory para iniciar sesión en el iDRAC6."

También puede iniciar en el iDRAC6 por medio de la tarjeta inteligente. Para obtener más información, consulte "Inicio de sesión en el iDRAC6 por medio de la tarjeta inteligente".

NOTA: El servidor de Windows 2008 Active Directory admite sólo una cadena de <nombre_de usuario>@<nombre_de_dominio> con un máximo de 250 caracteres.

Preguntas frecuentes

Mi inicio de sesión en Active Directory falló, ¿cómo puedo solucionar este problema?

iDRAC6 proporciona una herramienta de diagnóstico desde la interfaz basada en web. Inicie sesión como usuario local con privilegios de administrador en la interfaz basada en web. Navegue hasta **Acceso remoto**→ **Configuración**→ A**ctive Directo**ry. Desplácese hasta la parte inferior de la página de **Configuración y administración de Active Directory**, y haga clic en **Configurar Pruebay**. Ingrese un nombre de usuario y una contraseña de prueba y luego haga clic en **Iniciar prueba**. iDRAC6 ejecuta la prueba paso a paso y muestra el resultado de cada paso. También se registra un resultado detallado de prueba para ayudarlo a resolver los problemas. Haga clic en la lengüeta **Active Directory** para regresar a la página **Configuración y administración de Active Directory** . Desplácese hasta la parte inferior de la página y haga clic en **Configurar Active Directory** para cambiar su configuración y ejecute la prueba nuevamente hasta que la prueba pase el paso de autorización.

Activé la validación del certificado, pero no puedo iniciar sesión en Active Directory. Ejecuté los diagnósticos de la GUI y los resultados de la prueba muestran el siguiente mensaje de error:

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.

(ERROR: No se puede establecer conexión con el servidor LDAP, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:error en la validación del certificado: verifique que se ha cargado en el iDRAC el certificado correcto de la Autoridad de certificados (CA). Verifique también si la fecha del iDRAC se encuentra dentro del período válido de los certificados y si la dirección del controlador de dominio configurada en iDRAC concuerda con el sujeto del certificado del servidor de directorio.)

¿Cuál puede ser el problema y cómo puedo solucionarlo?

Si la validación del certificado está activada, iDRAC6 utiliza el certificado de CA cargado para verificar el certificado del servidor de directorio cuando iDRAC6 establece la conexión SSL con el servidor de directorio. Los motivos más frecuentes de error en la validación del certificado son:

1. La fecha del iDRAC6 no se encuentra dentro del período válido del certificado del servidor o del certificado de CA. Verifique el tiempo del iDRAC6 y el período válido de su certificado.

2. Las direcciones del controlador de dominio configuradas en el iDRAC6 no concuerdan con el sujeto o con el nombre alternativo del sujeto del certificado del servidor de directorio. Si utiliza una dirección IP, lea la siguiente pregunta y respuesta. Si utiliza FQDN, asegúrese de que utiliza el FQDN del controlador de dominio, no el dominio, por ejemplo, nombredeservidor.ejemplo.com en lugar de ejemplo.com.

Estoy usando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?

Verifique el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Generalmente, Active Directory utiliza el nombre de host, no la dirección IP, del controlador de dominio en el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Puede solucionar el problema de diferentes maneras:

1. Configure el nombre del host (FQDN) del controlador de dominio como las *direcciones de controlador de dominio* en el iDRAC6 para que coincidan con el

Sujeto o el Nombre alternativo de sujeto del certificado del servidor.

2. Vuelva a emitir el certificado del servidor de forma tal que use una dirección IP en el campo Sujeto o Nombre alternativo de sujeto que concuerde con la dirección IP configurada en el iDRAC6.

3. Desactive la validación de certificado si prefiere confiar en este controlador de dominio sin validación de certificado durante el enlace con SSL.

Utilizo un esquema ampliado en un entorno de múltiples dominios, ¿cómo debo configurar las direcciones del controlador de dominio?

Debe usar el nombre del host (FQDN) o la dirección IP de los controladores de dominio donde reside el objeto iDRAC6.

¿Cuándo necesito configurar una dirección de Catálogo global?

Si utiliza un esquema ampliado, no se utiliza la dirección del Catálogo global.

Si está utilizando un esquema estándar, y los usuarios y grupos de funciones pertenecen a dominios distintos, debe configurar las direcciones de catálogo global. En este caso, sólo puede utilizar el Grupo universal.

Si está utilizando un esquema estándar, y todos los usuarios y grupos de funciones se encuentran en el mismo dominio, no son necesarias las direcciones de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

iDRAC6 primero se conecta a las direcciones del controlador de dominio configuradas, si el usuario y los grupos de funciones, se guardarán los privilegios.

Si se configuran direcciones de controlador global, iDRAC6 continúa consultando el Catálogo global. Si se recuperan privilegios adicionales del Catálogo global, estos privilegios se acumularán.

¿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*, iDRAC6 efectúa una CONEXIÓN A LDAP sólo para ayudar a aislar el problema, pero no se vincula a LDAP con una conexión insegura.

¿Por qué iDRAC6 activa la validación del certificado de forma predeterminada?

iDRAC6 aplica fuertes medios de seguridad para asegurar la identidad del controlador de dominio al que se conecta iDRAC6. Sin la validación de certificados, un pirata informático podría falsificar un controlador de dominio y controlar la conexión SSL. Si decide confiar en todos los controladores de dominio en su barrera de seguridad sin la validación de certificados, puede desactivarla por medio de la GUI o CLI.

¿iDRAC6 es compatible con el nombre NetBIOS?

No en esta versión.

¿Qué debo verificar si no puedo iniciar sesión en iDRAC6 con Active Directory?

Puede diagnosticar el problema haciendo clic en Comprobar configuración en la parte inferior de la página Configuración y administración de Active Directory en la interfaz basada en web del iDRAC6. Luego, puede solucionar el problema detallado en el resultado de la prueba. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

La mayoría de los problemas se explican en esta sección; sin embargo, por lo general debe verificar lo siguiente:

1. Asegúrese de usar el nombre de dominio de usuario correcto durante un inicio de sesión y no el nombre de NetBIOS.

2. Si tiene una cuenta de usuario local de iDRAC6, inicie sesión en el iDRAC6 usando las credenciales locales.

   Después de haber iniciado sesión:

   a. Asegúrese de haber marcado la casilla **Activar Active Directory** en la página **Configuración de Active Directory** de iDRAC6.

   b. Asegúrese de que la configuración del DNS sea correcta en la página Configuración de la red de iDRAC6.

   c. Asegúrese de que haya cargado el certificado correcto de CA de raíz de Active Directory en iDRAC6. Asegúrese de que el tiempo del iDRAC6 se encuentre dentro del período de validez del certificado de CA.

   d. Si está utilizando el esquema ampliado, asegúrese de que el **Nombre del i**DRAC6 y el **Nombre de dominio del i**DRAC6 coincidan con la configuración del entorno de Active Directory.

      Si está utilizando el esquema ampliado, asegúrese de que el **Nombre del grupo** y el **Nombre del dominio del grupo** coincidan con la configuración del entorno de Active Directory.

3. Verifique los certificados de controlador de dominio SSL para asegurarse de que el tiempo del iDRAC6 está dentro del plazo de vigencia del certificado.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la autenticación de tarjeta inteligente

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

El iDRAC6 admite la característica autenticación de dos factores (TFA, por sus siglas en inglés) si se activa el **Inicio de sesión de tarjeta inteligente**.

Los esquemas tradicionales de autenticación usan nombres de usuario y contraseñas para autenticar a los usuarios. Esto proporciona una seguridad mínima.

La TFA, por el contrario, proporciona un mayor nivel de seguridad al proporcionarle al usuario dos factores de autenticación: lo que sabe y lo que tiene; lo que tiene es una tarjeta inteligente, un dispositivo físico, y lo que sabe, un código secreto como una contraseña o un NIP.

La autenticación de dos factores requiere que los usuarios verifiquen su identidad al proporcionar *ambos* factores.

Configuración del inicio de sesión de la tarjeta inteligente en iDRAC6

Para activar la característica del inicio de sesión inteligente en iDRAC6 desde la interfaz web, vaya a **Acceso remoto**→ **Configuración**→ **Tarjeta inteligente y seleccione Activar**.

Si usted:

- **Activa** o Activa con racadm remota, se le pedirán datos de inicio de sesión de tarjeta inteligente en los intentos de inicio de sesión subsiguientes a través de la interfaz web.

  Cuando selecciona **Activar**, todas las interfaces fuera de banda de la interfaz de línea de comandos (CLI) , como la telnet, SSH, serial, RACADM remota, y IPMI en LAN, están desactivadas porque estos servicios solo admiten autenticación de un solo factor.
  Cuando seleccione **Activar con racadm remota**, se desactivarán todas las interfaces fuera de banda de CLI, salvo RACADM remota.

  NOTA: Dell recomienda que el administrador de DRAC6 utilice la opción **Activar con racadm remota** únicamente para acceder a la interfaz web del DRAC6 a fin de ejecutar secuencias de comandos por medio de los comandos de RACADM remota. Si el administrador no necesita usar RACADM remota, Dell recomienda que se utilice la opción **Activar** para el inicio de sesión de tarjeta inteligente. Asimismo, compruebe que la configuración de usuario local del DRAC6 y/ o la configuración de Active Directory estén completas antes de activar el **Inicio de sesión de tarjeta inteligente**.

- **Desactivar** la configuración de la tarjeta inteligente (predeterminado). Esta sección desactiva la característica de inicio de sesión de la tarjeta inteligente y la siguiente vez que inicia sesión en la interfaz gráfica de iDRAC6, se le pedirá un Microsoft® Active Directory® o un nombre de usuario de sesión local y una contraseña, que es el cuadro de diálogo predeterminado para iniciar sesión en la interfaz web.
- **Activar comprobación de CRL para el inicio de sesión de tarjeta inteligente**, el certificado de iDRAC del usuario, que se descarga del servidor de distribución de la Lista de revocación de certificado (CRL) se revisa en la CRL para determinar si se ha revocado.

  NOTA: Los servidores de distribución de CRL aparecen en los certificados de tarjeta inteligente de los usuarios.

Configuración de usuarios de DRAC6 locales para inicio de sesión de tarjeta inteligente

Puede configurar que los usuarios iDRAC6 locales inicien sesión en el iDRAC6 usando la tarjeta inteligente. Diríjase a **Acceso remoto**→ **Configuración**→ **Usuarios**.

Sin embargo, antes de que el usuario pueda iniciar sesión en el DRAC6 con la tarjeta inteligente, usted debe cargar el certificado de tarjeta inteligente del usuario y el certificado de la CA (autoridad de certificados) de confianza para certificar el DRAC6.

Exportación del certificado de tarjeta inteligente

Puede obtener el certificado del usuario mediante la exportación del certificado de tarjeta inteligente por medio del software de administración de tarjetas (CMS), de la tarjeta inteligente a un archivo en el formato codificado Base64. Habitualmente, el CMS puede obtenerse del proveedor de la tarjeta inteligente. Este archivo codificado se debe cargar como certificado del usuario en el DRAC6. 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. Usted 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) del usuario en el certificado de la tarjeta inteligente.

NOTA: Para iniciar sesión en el DRAC6, el nombre de usuario que configuró en el DRAC6 debe ser exactamente igual que el Nombre principal de usuario (UPN) que figura en el certificado de tarjeta inteligente.

Por ejemplo, en caso que se haya emitido el certificado de tarjeta inteligente para el usuario, "usuario_muestra@domino.com", el nombre de usuario deberá configurarse como "usuario_muestra".

Configuración de usuarios de Active Directory para inicio de sesión de tarjeta inteligente

Para configurar los usuarios de Active Directory para que inicien sesión en el DRAC6 por medio de la tarjeta inteligente, el administrador del DRAC6 deberá configurar el servidor DNS, cargar el certificado de CA de Active Directory en el DRAC6 y activar el inicio de sesión de Active Directory. Consulte "Uso de iDRAC6 con Microsoft Active Directory" para obtener más información sobre cómo configurar usuarios de Active Directory.

NOTA: Si el usuario de la tarjeta inteligente está presente en el Active Directory, se requiere una contraseña de Active Directory junto con el NIP de la tarjeta inteligente. En versiones futuras, quizá no se requiera la contraseña del Active Directory.

Puede configurar Active Directory a partir del menú **Acceso remoto**→ **Configuración**→ **Active Directory**.

Configuración de la tarjeta inteligente

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Tarjeta inteligente**.
3. Configure los valores de inicio de sesión de tarjeta inteligente.

   La Tabla 8-1 contiene información sobre los valores de la página **Tarjeta inteligente**.
4. Haga clic en **Aplicar cambios**.

Tabla 8-1. Valores de la tarjeta inteligente

Valor	Descripción
Configurar inicio de sesión de tarjeta inteligente	• Desactivado: desactiva el inicio de sesión de tarjeta inteligente. Los inicios de sesión subsiguientes en la interfaz gráfica de usuario mostrarán la página normal de inicio de sesión. Todas las interfaces de línea de comandos fuera de banda, incluso Secure Shell (SSH), Telnet, serie y RACADM remota toman el valor predeterminado correspondiente. • Activado: activa el inicio de sesión de tarjeta inteligente. Después de aplicar los cambios, cierre sesión, inserte su tarjeta inteligente y después haga clic en **Iniciar sesión** para introducir el PIN de la tarjeta inteligente. La activación del inicio de sesión de tarjeta inteligente desactiva todas las interfaces fuera de banda de CLI, incluso SSH, Telnet, serie, RACADM remota e IPMI mediante LAN. • Activado con racadm remota: activa el inicio de sesión de tarjeta inteligente junto con RACADM remota. Todas las demás interfaces fuera de banda de la CLI se desactivan. **NOTA:** El inicio de sesión de la tarjeta inteligente requiere que se configuren usuarios locales del DRAC6 con los certificados correspondientes. Si se utiliza el inicio de sesión de tarjeta inteligente para que un usuario de Microsoft Active Directory inicie sesión, usted deberá asegurarse de configurar el certificado de usuario de Active Directory para dicho usuario. Puede configurar el certificado de usuario en la página **Usuarios**→i**Menú principal de usuario**.
Activar comprobación de CRL para el inicio de sesión de tarjeta inteligente	Esta comprobación está disponible únicamente para usuarios de inicio de sesión de Active Directory. 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. 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:** Usted debe configurar correctamente la dirección IP del servidor DNS en la página **Configuración**→ **Red** para que esta comprobación se realice correctamente

Inicio de sesión en el iDRAC6 por medio de la tarjeta inteligente

La interfaz web del iDRAC6 muestra la página de inicio de sesión de tarjeta inteligente de todos los usuario que fueron configurados para usar la tarjeta inteligente.

NOTA: Compruebe que la configuración de usuario local del iDRAC6 y/o la configuración de Active Directory esté completa antes de activar el inicio de sesión de tarjeta inteligente para el usuario.

NOTA: De acuerdo con la configuración del navegador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

1. Ingrese a la página web del iDRAC6 usando https.

   https://<*dirección IP*>

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<*dirección IP*>:<*número de puerto*>

   donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

   La página Inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.

   El iDRAC6 solicitará el NIP de la tarjeta inteligente.

3. Ingrese el NIP de la tarjeta inteligente para los usuarios locales de la tarjeta inteligente y si el usuario no fue creado localmente, iDRAC6 solicitará que se ingrese la contraseña para la cuenta del usuario en Active Directory.

NOTA: Si usted es un usuario de Active Directory para quien se ha seleccionado la opción **Activar comprobación de CRL para inicio de sesión de tarjeta inteligente**, el iDRAC6 intentará descargar la CRL y buscará en ella el certificado del usuario. El inicio de sesión por medio de Active Directory fallará si el certificado aparece como revocado en la CRL o si la CRL no se puede descargar por cualquier motivo.

Ahora está conectado al iDRAC6.

Inicio de sesión en el iDRAC6 mediante la autenticación con tarjeta inteligente de Active Directory

1. Inicie sesión en iDRAC6 usando https.

   https://<*dirección IP*>

   Si se ha modificado el número de puerto HTTPS predeterminado (puerto 443), escriba:

   https://<*dirección IP*>:<*número de puerto*>

   donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

   La página Inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.

   Se abrirá el cuadro de diálogo emergente para ingresar el PIN.

3. Introduzca el PIN y haga clic en **Aceptar**.

4. Ingrese la contraseña de Active Directory del usuario para autentificar la tarjeta inteligente y haga clic en **Aceptar**.

   De esta forma habrá iniciado sesión en el iDRAC6 con sus credenciales, tal como están definidas en Active Directory.

NOTA: Si el usuario de la tarjeta inteligente está presente en el Active Directory, se requiere una contraseña de Active Directory junto con el NIP de la tarjeta inteligente. En versiones futuras, quizá no se requiera la contraseña del Active Directory.

Identificación y resolución de problemas de del inicio de sesión de la tarjeta inteligente en iDRAC6

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Compruebe que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows®. Windows admite una cantidad limitada de proveedores de servicios criptográficos (CSP) de tarjetas inteligentes.

Consejo: como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y revise si Windows detecta la tarjeta inteligente y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

Imposible iniciar sesión en iDRAC6 local

Si un usuario de iDRAC6 local no puede iniciar sesión, revise si el nombre de usuario y los certificados de usuario que están cargados en el iDRAC6 han expirado. Los registros de rastreo del iDRAC6 pueden proporcionar mensajes importantes de registro relacionados con errores; sin embargo, los mensajes de error son, algunas veces, intencionalmente ambiguos por motivos de seguridad.

No se puede iniciar sesión en el iDRAC6 como usuario de Active Directory

Si no puede iniciar sesión en el iDRAC6 como usuario de Active Directory, trate de iniciar sesión en el iDRAC6 sin activar el inicio de sesión de tarjeta inteligente. Si ha activado la comprobación de CRL, intente iniciar sesión en Active Directory sin activar la comprobación de CRL. El registro de rastreo de iDRAC6 deberá proporcionar mensajes importantes si se presenta algún error de CRL.

También tiene la opción de desactivar el inicio de sesión de tarjeta inteligente a través de racadm local con el siguiente comando:

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la redirección de consola con interfaz gráfica de usuario

Acceso remoto integrado Dell™ Controladora 6 (iDRAC6) Versión 1.0 Guía del usuario

Esta sección proporciona información acerca de cómo usar la función de redirección de consola del iDRAC6.

Información general

La función de redirección de consola de iDRAC6 le permite tener acceso a la consola del servidor local de manera remota en modos de gráficos o de texto. Por medio de la redirección de consola, puede controlar uno o varios sistemas equipados con iDRAC6 desde una ubicación.

No es necesario ir personalmente a cada servidor para realizar todo el mantenimiento de rutina. En vez de eso, usted puede administrar los servidores desde donde se encuentre, desde su equipo de escritorio o desde su equipo portátil. También puede compartir la información con otros; de manera remota e instantánea.

Uso de redirección de consola

NOTA: Cuando usted abre una sesión de redirección de consola, el servidor administrado no indica que la consola ha sido redirigida.

NOTA: Si ya hay abierta una sesión de redirección de consola, desde la estación de administración al iDRAC6, al intentar abrir una nueva sesión desde la misma estación de administración a ese iDRAC6, se activará la sesión existente. No se generará una nueva sesión.

NOTA: Es posible abrir varias sesiones de redirección de consola desde una sola estación de administración hacia varias tarjetas de iDRAC6 simultáneamente.

La página **Redirección de consola** permite administrar el sistema remoto con el teclado, vídeo y mouse en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta característica puede ser usada junto con la característica de medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- Sólo se admite un máximo de cuatro sesiones simultáneas de redirección de consola. Todas las sesiones muestran la misma consola de servidor administrado simultáneamente.
- Sólo se puede abrir una sesión hacia un servidor remoto (iDRAC6) desde la misma consola cliente (estación de administración). Sin embargo, se pueden abrir varias sesiones hacia varios servidores remotos desde el mismo cliente.
- La sesión de redirección de consola no se deberá ejecutar desde un explorador web en el sistema administrado.
- Se requiere un ancho de banda disponible de red de 1 MB/s.

La primera sesión de redirección de consola hacia el iDRAC es una sesión de acceso completo. Si otro usuario solicita una sesión de redirección de consola, el primer usuario recibe una notificación y tiene la opción de rechazarla, **permitirla como sólo lectura** o **aprobarla**. El segundo usuario es notificado que otro usuario tiene el control. El primer usuario debe responder en treinta segundos o se rechazará el acceso al segundo usuario.

Todas las sesiones **permitidas como sólo lectura** se cierran automáticamente cuando finaliza la última sesión que tiene acceso completo.

Configuración de la estación de administración

Para usar la redirección de consola en la estación de administración, realice los siguientes procedimientos:

1. Instale y configure un explorador de web admitido. Consulte las siguientes secciones para obtener más información:
   - "Exploradores web admitidos"
   - "Configuración de un explorador de web admitido"

   NOTA: Debe instalarse Java Runtime Environment en la estación de administración para que funcione la función de redirección de consola.

2. Si utiliza Internet Explorer, asegúrese de que el navegador esté activado para descargar contenido cifrado de esta forma:
   - Desde Internet Explorer, vaya a Opciones o Configuración y seleccione **Herramientas**→ **Opciones de Internet**→ **Opciones avanzadas**.
   - Desplácese hasta la sección **Seguridad** y desmarque esta opción:

     No guardar las páginas cifradas en el disco.

3. Se recomienda que configure la resolución del monitor en 1280 x 1024 pixeles o más.

NOTA: Si tiene una sesión de redirección de consola activa y hay un monitor de menor resolución conectado con el iDRAC KVM, la resolución de la consola del servidor puede restablecerse si el servidor se selecciona en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iDRAC KVM, se cambiará de 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 la red para utilizar la "Conexión directa" en JavaWebStart: "Editar->Preferencias->General->Configuración de red" y elija "Conexión directa" en lugar de "Utilizar configuración del navegador".

Configuración de la redirección de consolaen la interfaz web del iDRAC6

Para configurar la redirección de consola en la interfaz web del iDRAC6, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **Consola / Medios**→ **Configuración** para configurar los ajustes de redirección de consola del iDRAC.
2. Configure las propiedades de la redirección de consola.La Tabla 9-1 describe la configuración de la redirección de consola.
3. Cuando termine, haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la Tabla 9-2.

Tabla 9-1. Propiedades de configuración de la redirección de consola

Propiedad	Descripción
Activado	Haga clic para activar o desactivar la Redirección de consola. **Seleccionado** indica que la redirección de consola está activada. **Deseleccionado** indica que la redirección de consola está desactivada. El valor predeterminado es **activado**.
N° máx. de sesiones	Muestra el número máximo posible de sesiones de redirección de consola, 1 a 4. Use el menú desplegable para cambiar el número máximo posible de sesiones de Redirección de consola. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de Consola activa. Este campo es de sólo lectura.
Puerto de presencia remota	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es **5900**.
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.**
Vídeo del servidor local activado	Si está seleccionado, indica que la salida al monitor iDRAC KVM está desactivada durante la redirección de consola. Esto garantiza que las tareas que realice usando **Redirección de consola** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte "Configuración y uso de medios virtuales".

Los botones que se muestran en la Tabla 9-2 están disponibles en la página de **configuración de la consola y los medios**.

Tabla 9-2. Botones de la página de configuración

Botón	Definición
Imprimir	Imprime la página
Actualizar	Vuelve a cargar la página **Configuración**
Aplicar cambios	Guarda los ajustes nuevos o modificados

Abrir una sesión de redirección de consola

Cuando abre una sesión de redirección de consola, la aplicación Dell™ Virtual KVM Viewer se inicia y aparece el escritorio del sistema remoto en el visor. Al usar la aplicación Virtual KVM Viewer, puede controlar las funciones de mouse y teclado del sistema remoto desde la estación de administración local.

Para abrir una sesión de redirección de consola en la interfaz web, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **Consola / Medios**→ **Configuración**.

2. Utilice la información en Tabla 9-3 para asegurarse de que una sesión de redirección de consola está disponible.

   Si desea volver a configurar los valores de propiedades que se muestran, consulte "Configuración de la redirección de consolaen la interfaz web del iDRAC6".

Tabla 9-3. Redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No (seleccionado/no seleccionado)
Cifrado de vídeo activado	Sí/No (seleccionado/no seleccionado)
N° máx. de sesiones	Muestra el número máximo de sesiones de redirección de consola admitidas
Sesiones activas	Muestra el número actual de sesiones activas de redirección de consola
Vídeo del servidor local activado	Estará deseleccionado si la consola local no ha sido desactivada. Si está seleccionado, no se puede tener acceso a la consola si la conexión local de iDRAC KVM está siendo utilizada como remota.
Puerto de presencia remota	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es 5900.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la redirección de consola, consulte "Configuración y uso de medios virtuales".

Los botones en Tabla 9-4 están disponibles en la página **Redirección de consola y Medios virtuales**.

Tabla 9-4. Botones de Redirección de consola y Medios virtuales

Botón	Definición
Actualizar	Actualiza la página **Configuración de la redirección de consola**
Iniciar el visor	Abre una sesión de redirección de consola en el sistema remoto de destino
Imprimir	Imprime la página **Configuración de la redirección de consola**

3. Si hay una sesión de redirección de consola disponible, haga clic en **Iniciar el visor**.

   NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

   NOTA: Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información en la ventana y haga clic en **Sí** para seguir.

   La estación de administración se conecta al iDRAC6 y la pantalla de escritorio del sistema remoto aparecerá en la aplicación iDRAC KVM Viewer.

4. Aparecerán dos apuntadores de mouse en la ventana del visor: uno para el sistema remoto y otro para el sistema local. Puede cambiar a un solo cursor al seleccionar la opción **Un solo cursor** en **Herramientas** en el menú del iDRAC KVM.

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver la pantalla de escritorio del servidor administrado y controlar las funciones de mouse y teclado desde la estación de administración. Cuando se conecta con el sistema remoto, Video Viewer se inicia en otra ventana.

NOTA: Si el servidor remoto está apagado, se visualizará el mensaje **Sin señal**.

Video Viewer proporciona varios ajustes de control, 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 Redirección de consola y Medios virtuales** .

Cuando comience una sesión de redirección de consola y aparezca el Video Viewer, es posible que deba sincronizar los apuntadores del mouse.

Desactivación o activación del vídeo del servidor local

Usted puede configurar el iDRAC6 para rechazar conexiones de iDRAC KMV por medio de la interfaz web del iDRAC6.

Si desea asegurarse de tener acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local *y volver a configurar el* **Número máximo de sesiones** a 1 en la **página de Redirección de consola**.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, no se desactivarán el monitor, teclado y mouse que están conectados al iDRAC KVM.

Para desactivar o activar la consola local, realice el procedimiento siguiente:

1. En la estación de administración, abra un explorador web admitido e inicie sesión en el iDRAC6. Consulte "Acceso a la interfaz web" para obtener más información.

2. Haga clic en **Sistema**→ **Consola / Medios**→ **Configuración**.

3. Para desactivar (apagar) el vídeo local en el servidor, desmarque la casilla de verificación **Vídeo del servidor local activado** en la página de **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 de verificación **Vídeo del servidor local activado** en la página de **Configuración**, y luego haga clic en **Aplicar**.

Preguntas frecuentes

La Tabla 9-5 contiene las preguntas y respuestas frecuentes.

Tabla 9-5. Uso de la redirección de consola: Preguntas frecuentes

Pregunta	Respuesta
¿Se puede iniciar una nueva sesión de vídeo de consola remota cuando el vídeo local del servidor está apagado?	Sí.
¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del vídeo local?	Esto brinda al usuario local la oportunidad de realizar alguna acción antes de que el vídeo se apague.
¿Hay algún retraso al encender el vídeo local?	No, después de que el iDRAC6 recibe la solicitud de **encendido** del vídeo local, este último se enciende instantáneamente.
¿El usuario local también puede apagar el vídeo?	Cuando la consola local está desactivada, el usuario local no puede encender 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.
¿Cuáles son los privilegios necesarios para que un usuario de iDRAC6 active o desactive el vídeo del servidor local?	Cualquier usuario con privilegios de configuración del iDRAC6 puede activar o desactivar la consola local.
¿Cómo se puede ver el estado actual del vídeo del servidor local?	El estado se muestra en la página **Configuración de redirección de consola** de la interfaz web del iDRAC6. El comando **racadm getconfig -g cfgRacTuning** de la CLI de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**.
No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024. Pruebe utilizar las barras de desplazamiento también en el cliente del iDRAC KVM.
La ventana de la consola no es legible.	El visor de la consola en Linux requiere de un conjunto de caracteres UTF-8. Revise la configuración regional y, de ser necesario, restablezca el conjunto de caracteres.
¿Por qué no se sincroniza el mouse en la consola de texto de Linux?	El KVM virtual necesita 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 el mouse adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de redirección de consola. Asegúrese de que la opción **Un solo cursor** en **Herramientas** que aparece en el menú del iDRAC KVM esté seleccionada en el iDRAC KVM cliente.
¿Por qué no puedo usar un teclado o mouse mientras instalo un sistema operativo de Microsoft® de manera remota por medio de la redirección de consola del iDRAC6?	Cuando instala de manera remota un sistema operativo Microsoft admitido en un sistema con la redirección de consola habilitada en el BIOS, aparece un mensaje de conexión de EMS que le pide que seleccione **Aceptar** para poder continuar. Usted no puede usar el mouse para seleccionar **Aceptar** de manera remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la redirección de consola en el BIOS. Microsoft genera este mensaje para avisar al usuario que la redirección de consola está activada. Para asegurar que este mensaje no aparece, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Núm de mi estación de administración no muestra el estado de Bloq Núm en el servidor remoto?	Cuando se accede por medio de 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 Núm depende de la configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Núm en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.

sesión de redirección de consola desde el host local?	
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, ambos tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?	Dell recomienda una conexión de 5 MB/s para un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la redirección de consola?	Se requiere que la estación de administración tenga un procesador Intel® Pentium III a 500 MHz con al menos 256 MB de RAM.
¿Por qué veo un mensaje de **Sin señal** dentro de la aplicación iDRAC KVM Video Viewer?	Es posible que vea este mensaje porque el plugin de iDRAC Virtual KVM no recibe el vídeo del escritorio del servidor remoto. Generalmente, este comportamiento puede ocurrir cuando el servidor remoto está apagado. Ocasionalmente, el mensaje puede aparecer porque ocurrió una falla con la recepción del vídeo del escritorio del servidor remoto.
¿Por qué veo un mensaje de **Fuera de rango** dentro de la aplicación iDRAC KVM Video Viewer?	Es posible que vea este mensaje porque un parámetro necesario para capturar el vídeo esté fuera del rango mediante el cual iDRAC puede capturar el vídeo. Los parámetros como la resolución de pantalla o la frecuencia de actualización que estén muy elevados provocarán una condición de fuera de rango. Por lo general, el rango máximo de parámetros se configura por limitaciones físicas como el tamaño de la memoria de vídeo o el ancho de banda.

Regresar a la página de contenido

Regresar a la página de contenido

Controladora de Acceso remoto integrado Dell 6 (iDRAC6) Versión 1.0 Guía del usuario

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.

Marzo 2009 Rev. A00

Regresar a la página de contenido