Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

Descripción de iDRAC
Configuración del iDRAC
Configuración de la estación de administración
Configuración del servidor administrado
Configuración de iDRAC por medio de la interfaz web
Uso de iDRAC con Microsoft Active Directory
Uso de la redirección de consola con interfaz gráfica de usuario
Configuración y uso de medios virtuales
Uso de la interfaz de línea de comandos de RACADM local
Uso de la interfaz de línea de comandos de SM-CLP de iDRAC
Instalación del sistema operativo por medio de iVM-CLI
Uso de la utilidad de configuración del iDRAC
Recuperación y solución de problemas del servidor administrado
Descripción de subcomandos de RACADM
Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC
Equivalencias de RACADM y SM-CLP
Glosario

Notas y avisos

NOTA: Una NOTA indica información importante que ayuda a hacer mejor uso del equipo.

AVISO: Un AVISO indica la posibilidad de daños al hardware o pérdida de datos y le explica cómo evitar el problema.

Marzo de 2008 Rev. A01

Regresar a la página de contenido

Descripción de subcomandos de RACADM

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- help
- config
- getconfig
- getssninfo
- getsysinfo
- getractime
- setniccfg
- getniccfg
- getsvctag
- racreset
- racresetcfg
- serveraction
- getraclog
- clrraclog
- getsel
- clrsel
- gettracelog
- sslcsrgen
- sslcertupload
- sslcertdownload
- sslcertview
- testemail
- testtrap
- vmdisconnect

Esta sección proporciona descripciones de los subcomandos disponibles en la interfaz de línea de comandos de RACADM.

---

help

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

Tabla A-1. Comando help

Comando	Definición
help	Enumera 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 usa el comando **racadm** junto con una descripción de una línea. También puede escribir un subcomando después de **help** para obtener la sintaxis de un subcomando específico.

Salida

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

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

Interfaces admitidas

- RACADM local

---

config

La 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

La tabla A-3 describe 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 especificado 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 establecer.
-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 "nombrado".
-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 muestra el número de línea y una breve descripción del error. No se realizan las operaciones de escritura en el iDRAC. Esta opción es sólo un control.

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 inválido, u otros miembros inválidos de la base de datos
- Fallas de la CLI de RACADM

Este subcomando genera una indicación de cuántos objetos de configuración que se escribieron, del total de objetos, estaban en el archivo **.cfg**.

Ejemplos

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

  Establece el parámetro de configuración (objeto) **cfgNicIpAddress** en el valor 10.35.10.110. 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

La tabla A-4 describe las opciones del subcomando **getconfig**.

NOTA: La opción **-f** sin que se especifique un archivo mostrará el contenido del archivo en la pantalla de 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 usado 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 utilizar. 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 aquí mediante el valor del índice; no mediante un valor "nombrado".
-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 inválido, u otros miembros inválidos 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 están contenidos 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

La tabla A-5 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 se aplica)
- Tipo de sesión (por ejemplo, SSH o Telnet)
- Consolas en uso (por ejemplo, medios virtuales o un conmutador KVM virtual)

Interfaces admitidas

- RACADM local

Entrada

La tabla A-6 describe 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 se imprime cuando se especifica esta opción.

Ejemplos

- `racadm getssninfo`

La tabla A-7 ofrece un ejemplo del mensaje de salida generado por el 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	Virtual KVM

- `racadm getssninfo -A`

  `"root" 143.166.174.19 "Telnet" "NONE"`

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "NONE"`

- `"juan" "143.166.174.19" "GUI" "NONE"`

---

getsysinfo

La tabla A-8 describe las opciones del 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

La tabla A-9 describe 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 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

La tabla A-10 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

Sin opciones, el subcomando **getractime** muestra el tiempo en un formato legible común.

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

UNIX.

Salida

El subcomando **getractime** muestra la 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

La tabla A-11 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 se realizó satisfactoriamente, el subcomando **setniccfg** mostrará un mensaje de error correspondiente. Si se realiza satisfactoriamente, aparecerá un mensaje.

Interfaces admitidas

- RACADM local

---

getniccfg

La tabla A-12 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 se ejecuta satisfactoriamente, el subcomando **getniccfg** mostrará un 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

La tabla A-13 describe el subcomando **getsvctag**.

Tabla A-13. getsvctag

Subcomando	Definición
getsvctag	Muestra una 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 se muestra como a continuación:

```
Y76TP0G
```

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

Interfaces admitidas

- RACADM local

---

racreset

La tabla A-14 describe el subcomando **racreset**.

Tabla A-14. racreset

Subcomando	Definición
racreset	Restablece el iDRAC.

AVISO: Cuando usted ejecuta un subcomando racreset, es posible que el iDRAC tarde hasta un minuto en regresar a un estado en el que se pueda utilizar.

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

La tabla A-15 describe el subcomando **racresetcfg**.

Tabla A-15. racresetcfg

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

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 original 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

La tabla A-16 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. La tabla A-17 describe 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 anterior del sistema para apagar y luego 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

Si la operación solicitada no pudo realizarse, el subcomando **serveraction** mostrará un mensaje de error, o bien, un mensaje de ejecución satisfactoria si la operación se completó satisfactoriamente.

Interfaces admitidas

- RACADM local

---

getraclog

La tabla A-18 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 cuenta] [-s anotación_de_inicio] [-m]
```

Descripción

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

NOTA: Si no se especifican opciones, se muestra todo el registro.

A continuación, se muestran las opciones que permiten que el comando **getraclog** lea 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

La pantalla predeterminada del mensaje de salida muestra el número de anotación, la fecha y 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

La tabla A-20 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 cuenta] [-s cuenta] [-m]
```

Descripción

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

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

NOTA: Si no se especifican argumentos, se muestra 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

La pantalla predeterminada del mensaje de salida muestra el número de anotación, la fecha y hora, la gravedad 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

La tabla A-22 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 count] [-s startrecord] [-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

La pantalla predeterminada del mensaje de salida muestra el número de anotación, la fecha y 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

La tabla A-24 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 utilizar para generar una CSR y descargar el archivo al sistema de archivos local del cliente. La CSR se puede usar para crear un certificado SSL personalizado que puede ser usado para transacciones de SSL en el RAC.

Opciones

La tabla A-25 describe las opciones del subcomando **sslcsrgen**

Tabla A-25. Opciones del subcomando sslcsrgen

Opción	Descripción
-g	Genera una nueva CSR.
-s	Genera el estado de un proceso de generación de CSR (generación en progreso, activa o ninguna).
-f	Especifica el nombre de archivo de la ubicación <*nombre_de_archivo*>, donde la CSR será descargada.

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

Si no se especifican opciones, de manera predeterminada se generará y descargará una CSR en el sistema de archivos local como **sslcsr**. 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** genera uno de los siguientes códigos de estado:

- La CSR fue generada satisfactoriamente.
- La CSR no existe.
- Generación de CSR en progreso.

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

Ejemplos

```
racadm sslcsrgen -s
```

o

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

Interfaces admitidas

- RACADM local

sslcertupload

La tabla A-26 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

La tabla A-27 describe 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 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** genera `0` cuando es satisfactorio y un número diferente a cero cuando no es satisfactorio.

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertdownload

La tabla A-28 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

La tabla A-29 describe 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 especifican la opción **-f** o el nombre del archivo, se seleccionará el archivo **sslcert** en el directorio actual.

El comando **sslcertdownload** genera `0` cuando es satisfactorio y un número diferente a cero cuando no es satisfactorio.

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertview

La tabla A-30 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

La tabla A-31 describe las opciones del subcomando **sslcertview**

Tabla A-31. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado que se va a mostrar, ya sea el certificado de Microsoft Active Directory o el certificado del 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

La tabla A-32 describe el subcomando **testemail**.

Tabla A-32. Configuración de testemail

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

Sinopsis

```
racadm testemail -i <índice>
```

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
Activar la alerta	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Establecer la dirección de correo electrónico de destino	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 usuario1@mi_empresa.com
Establecer 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."
Comprobar que la dirección IP de SNMP está correctamente configurada	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 192.168.0.152
Ver los valores actuales de alerta de correo electrónico	racadm getconfig -g cfgEmailAlert -i *<índice>*

	donde *<índice>* es un número de 1 a 4

Opciones

La tabla A-34 describe las opciones del subcomando **testemail**.

Tabla A-34. Opción del subcomando testemail

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

Salida

Ninguna.

Interfaces admitidas

- RACADM local

---

testtrap

La tabla A-35 describe el subcomando **testtrap**.

Tabla A-35. testtrap

Subcomando	Descripción
testtrap	Prueba la función de alertas de capturas SNMP del iDRAC.

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

El subcomando **testtrap** prueba la función 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 del grupo **cfgIpmiPet**.

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

Acción	Comando
Activar la alerta	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
Establecer la dirección IP de correo electrónico de destino	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
Ver los valores actuales de la captura de prueba	racadm getconfig -g cfgIpmiPet -i <índice> donde *<índice>* es un número de 1 a 4

Entrada

La tabla A-37 describe las opciones del subcomando **testtrap**

Tabla A-37. Opciones del subcomando testtrap

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

Interfaces admitidas

- RACADM local

---

vmdisconnect

La tabla A-38 describe el subcomando **vmdisconnect**.

Tabla A-38. vmdisconnect

Subcomando	Descripción
vmdisconnect	Cierra todas las conexiones de medios virtuales de iDRAC desde los clientes remotos.

Sinopsis

```
racadm vmdisconnect
```

Descripción

El subcomando **vmdisconnect** permite que un usuario desconecte la sesión de medios virtuales de otro usuario. Una vez desconectada, la interfaz web reflejará el estado de conexión correcto. Este subcomando sólo está disponible a través del uso de RACADM de manera local.

El subcomando **vmdisconnect** habilita a un usuario del iDRAC para que desconecte todas las sesiones de medios virtuales activas. Las sesiones de medios virtuales activas pueden mostrarse en la interfaz web de RAC o mediante el subcomando **getsysinfo** de RACADM.

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 con firmware versión 1.00

- Caracteres que se pueden mostrar
- idRacInfo
- cfgLanNetworking
- cfgUserAdmin
- cfgEmailAlert
- cfgSessionManagement
- cfgSerial
- cfgRacTuning
- ifcRacManagedNodeOs
- cfgRacSecurity
- cfgRacVirtual
- cfgActiveDirectory
- cfgStandardSchema
- cfgIpmiSol
- cfgIpmiLan
- cfgIpmiPef
- cfgIpmiPet

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 están limitados al uso de caracteres ASCII que se puedan mostrar, excepto en los casos en los que se indique lo contrario.

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen los siguientes:

```
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

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 firmware del RAC. Por ejemplo, "05.12.06".

Descripción

Cadena que contiene la versión de compilación del producto actual.

idRacName (sólo lectura)

Valores legales

Cadena de hasta 15 caracteres ASCII.

Predeterminado

iDRAC

Descripción

Un usuario asigna un nombre 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 254 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 nombres de dominio totalmente calificados (FQDN) de 64 bytes o menos.

Predeterminado

""

Descripción

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

cfgDNSRacName (lectura / escritura)

Valores legales

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

NOTA: Algunos 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 es válido sólo si **cfgDNSRegisterRac** se establece en 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 desde el servidor DHCP en la red.

cfgDNSServer1 (lectura/escritura)

Valores legales

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

Descripción

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

NOTA: Se pueden asignar valores idénticos a **cfgDNSServer1** y **cfgDNSServer2** mientras se intercambian direcciones.

cfgDNSServer2 (Lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

Recupera la dirección IP utilizada por el servidor DNS 2. Este parámetro es válido sólo si **cfgDNSServersFromDHCP** se establece en 0 (FALSO).

NOTA: Se pueden asignar valores idénticos a **cfgDNSServer1** y **cfgDNSServer2** 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 será configurable si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSO).

Valores legales

Una cadena que represente 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 que la dirección IP estática se que se va a asignar al RAC. Esta propiedad es válida sólo si **cfgNicUseDhcp** se establece en **0** (FALSO).

cfgNicNetmask (lectura/escritura)

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

Valores legales

Una cadena que represente 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 es válida sólo si **cfgNicUseDhcp** se establece en **0** (FALSO).

cfgNicGateway (lectura/escritura)

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

Valores legales

Una cadena que represente una dirección IP válida de puerta de enlace. 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 sólo si **cfgNicUseDhcp** se establece en **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 en **0** (FALSO), la dirección IP estática, la máscara de subred y la puerta de enlace se asignan a partir de las propiedades **cfgNicIpAddress**, **cfgNicNetmask** y **cfgNicGateway**.

cfgNicMacAddress (sólo lectura)

Valores legales

Una cadena que represente la dirección MAC del NIC 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 proporciona la información de configuración acerca de los usuarios que tienen permiso de acceder al RAC por medio de las interfaces remotas disponibles.

Se permiten hasta 16 instancias del grupo de usuarios. 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
Configuración del iDRAC	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a la redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Ejemplos

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

Tabla B-2. Ejemplos de máscaras de bit para privilegios del usuario

Privilegio(s) de 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 tiene permiso de iniciar sesión en el RAC, acceder a los medios virtuales y acceder a la redirección de consola.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lectura/escritura)

Valores legales

Cadena. Número máximo 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 contener / (diagonal), \ (diagonal invertida), . (punto), @ (arroba) 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 ser vistas o mostradas después que se haya escrito la propiedad.

cfgUserAdminEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva a un usuario individual.

cfgUserAdminSolEnable

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

---

cfgEmailAlert

Este grupo contiene parámetros para configurar la capacidad de alertas 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

1–4

Predeterminado

Este parámetro se llena en base a 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

El formato de dirección de correo electrónico, con una longitud máxima de 64 caracteres ASCII.

Predeterminado

""

Descripción

La dirección de correo electrónico de la fuente de alerta.

cfgEmailAlertCustomMsg

Valores legales

Cadena. Número máximo de caracteres = 32.

Predeterminado

""

Descripción

Especifica un mensaje personalizado que se envía junto con la alerta.

---

cfgSessionManagement

Este grupo contiene parámetros para configurar el número 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

1 – 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

60 – 1920

Predeterminado

300

Descripción

Define el tiempo de espera del servidor web. Esta propiedad establece la cantidad de tiempo en segundos que se permite que una conexión permanezca sin actividad (sin introducción de datos por parte del usuario). Si se llega al límite de tiempo establecido por esta propiedad, la sesión se cancelará. Los cambios de este valor no afectan la sesión actual; usted debe cerrar sesión y volver a iniciar sesión para que la nueva configuración surta efecto.

La expiración de una sesión de servidor web hace que se cierre la sesión actual.

cfgSsnMgtSshIdleTimeout (lectura/escritura)

Valores legales

0 (Sin expiración de tiempo)

60 – 1920

Predeterminado

300

Descripción

Define el tiempo de espera en inactividad de Secure Shell. Esta propiedad establece la cantidad de tiempo en segundos que se permite que una conexión permanezca sin actividad (sin introducción de datos por parte del usuario). Si se llega al límite de tiempo establecido por esta propiedad, la sesión se cancelará. Los cambios de este valor no afectan la sesión actual; usted debe cerrar sesión y volver a iniciar sesión para que la nueva configuración surta efecto.

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

```
Warning: Session no longer valid, may have timed out
```

```
(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 Secure Shell.

cfgSsnMgtTelnetIdleTimeout (lectura/escritura)

Valores legales

0 (Sin expiración de tiempo)

60 – 1920

Predeterminado

300

Descripción

Define el tiempo de espera en inactividad de Telnet. Esta propiedad establece la cantidad de tiempo en segundos que se permite que una conexión permanezca sin actividad (sin introducción de datos por parte del usuario). Si se llega al límite de tiempo establecido por esta propiedad, la sesión se cancelará. Los cambios de este valor no afectan la sesión actual (usted debe cerrar sesión y volver a iniciar sesión para que la nueva configuración surta efecto).

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

```
Warning: Session no longer valid, may have timed out
```

```
(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) interfaz 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

10 – 65535

Predeterminado

80

Descripción

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

cfgRacTuneHttpsPort (lectura / escritura)

Valores legales

10 – 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 en formato de dirección IP. Por ejemplo, 192.168.0.44.

Predeterminado

192.168.1.1

Descripción

Especifica la sucesión de bits de dirección IP aceptable en las posiciones que se indican con los unos (1) en la propiedad de máscara de rango (**cfgRacTuneIpRangeMask**).

cfgRacTuneIpRangeMask

Valores legales

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

Predeterminado

255.255.255.0

Descripción

Cadena en formato de 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

2 – 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

10 – 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

10 – 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

1 – 65535

Predeterminado

22

Descripción

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

cfgRacTuneTelnetPort (lectura / escritura)

Valores legales

1 – 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 la codificación de vídeo en una sesión de redirección de consola.

cfgRacTuneConRedirPort (lectura / escritura)

Valores legales

1 – 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

1 – 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 (Activada)

0 (Desactivada)

Predeterminado

1

Descripción

Activa (enciende) o desactiva (apaga) el vídeo del servidor 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 (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 255.

Predeterminado

""

Descripción

El nombre de host del servidor administrado.

ifcRacMnOsOsName (lectura/escritura)

Valores legales

Cadena. Número máximo 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** de RACADM para obtener más información acerca de la generación de solicitudes de firma de certificados.

cfgSecCsrCommonName (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica el nombre común (CN) de la CSR.

cfgSecCsrOrganizationName (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica la unidad de organización (OU) de la CSR.

cfgSecCsrLocalityName (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica la localidad (L) de la CSR.

cfgSecCsrStateName (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrCountryCode (lectura/escritura)

Valores legales

Cadena. Número máximo de caracteres = 2.

Predeterminado

""

Descripción

Especifica el código del país (CC) de la CSR

cfgSecCsrEmailAddr (lectura/escritura)

Valores legales

Cadena. Número máximo 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 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 disquete, 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 establece un valor de **0** para este objeto, hará que los dispositivos se desconecten del bus USB.

NOTA: Para habilitar todos los cambios, debe reiniciar su sistema.

cfgVirAtapiSrvPort (lectura / escritura)

Valores legales

1 – 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 no utilizado entre 0 y 65535 en decimales.

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 cuando el servidor host se reinicia, la función intentará iniciar a partir de los dispositivos de medios virtuales; si los medios adecuados están 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 la letra de unidad C: o letras posteriores del alfabeto durante la enumeración. Cuando se define como 1, los sistemas operativos Windows detectarán la unidad de disco flexible virtual como unidad de disco flexible. Los sistemas operativos Windows asignarán la 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 que se pueda imprimir, sin espacios en blanco. La longitud se limita a 254 caracteres.

Predeterminado

""

Descripción

El dominio de Active Directory en que reside el DRAC.

cfgADRacName (lectura / escritura)

Valores legales

Cualquier cadena de texto que se pueda imprimir, sin espacios en blanco. La longitud se limita a 254 caracteres.

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, usted debe tener permiso para **Configurar el iDRAC**.

Valores legales

15 – 300

Predeterminado

120

Descripción

Especifica el número de segundos que se debe esperar para completar las solicitudes de autentificación de Active Directory antes de finalizar.

cfgADRootDomain, (lectura / escritura)

Valores legales

Cualquier cadena de texto que se pueda imprimir, sin espacios en blanco. La longitud se limita a 254 caracteres.

Predeterminado

""

Descripción

Dominio raíz del bosque del dominio.

cfgADSpecifyServerEnable (lectura / escritura)

Valores legales

1 ó 0 (verdadero o falso)

Predeterminado

0

Descripción

1 (verdadero) le 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 usará con 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 de 1 a 5.

Descripción

El índice del grupo de funciones según se registró en Active Directory.

cfgSSADRoleGroupName (lectura/escritura)

Valores legales

Cualquier cadena de texto que se pueda imprimir, sin espacios en blanco. La longitud se limita a 254 caracteres.

Predeterminado

(en blanco)

Descripción

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

cfgSSADRoleGroupDomain (lectura/escritura)

Valores legales

Cualquier cadena de texto que se pueda imprimir, sin espacios en blanco. La longitud se limita a 254 caracteres.

Predeterminado

(en blanco)

Descripción

El dominio de Active Directory en el que reside el grupo de funciones.

cfgSSADRoleGroupPrivilege (lectura/escritura)

Valores legales

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

Predeterminado

(en blanco)

Descripción

Utilice los números de máscara de bit en la tabla B-3 para establecer privilegios de autoridad basados en funciones para un Grupo de funciones.

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

Privilegio del grupo de funciones	Máscara de bits
Inicio de sesión en iDRAC	0x00000001
Configuración del iDRAC	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a la 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 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 serie en la LAN.

cfgIpmiSolAccumulateInterval (lectura/escritura)

Valores legales

1 – 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 se basa en incrementos de 5 ms a partir de 1.

cfgIpmiSolSendThreshold (lectura/escritura)

Valores legales

1 – 255

Predeterminado

255

Descripción

El valor límite del umbral de la 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 máximo de privilegios que se requiere para tener acceso a la IPMI en la LAN.

cfgIpmiLanAlertEnable (lectura/escritura)

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

Activa o desactiva el envío global de alertas por correo electrónico. Esta propiedad suprime todas las propiedades de activación y desactivación del envío de alertas individuales 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 usa para configurar los filtros de sucesos de 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. Número máximo 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

1 – 17

Predeterminado

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

Descripción

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

cfgIpmiPefAction (lectura/escritura)

Valores legales

0 (Ninguna)

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 específico de sucesos de plataforma.

---

cfgIpmiPet

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

cfgIpmiPetIndex (lectura/escritura)

Valores legales

1 – 4

Predeterminado

El valor de índice adecuado.

Descripción

Identificador único del 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

Equivalencias de RACADM y SM-CLP

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

La tabla C-1 muestra una lista de los grupos y objetos de RACADM y, en donde corresponden, los lugares equivalentes de SM-SLP en el punto de acceso de administrabilidad de SM-CLP.

Tabla C-1. Equivalencias de RACADM y SM-CLP

Grupo 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	Cadena de hasta 254 caracteres.
cfgADRacDomain	oemdell_adracdomain	Cadena de hasta 254 caracteres.
cfgADRootDomain	oemdell_adrootdomain	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**
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	Cadena de hasta 254 caracteres.
cfgSSADRoleGroupDomain	oemdell_groupdomain	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 254 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**
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	Una cadena que represente la dirección IP de un servidor DNS.
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer2	dnsserveraddresses2	Una cadena que represente la dirección IP de un servidor DNS.
	/server1/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	**/server1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	Establezca el valor en 1 para activar la emulación de disco flexible. Valor predeterminado: **0**
cfgVirMediaAttached	enabledstate	Establezca el valor en 1 (RACADM)/VMEDIA_ATTACH (SM-CLP) para conectar 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**.
	/server1/sp1/oemdell_vmservice1/ptfintcp1	
	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**
	/server1/sp1/oemdell_vmservice1/tcendpt2	
	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	**/server1/sp1/oemdell_vmservice1/tcpendpt2**	
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 utilice 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 Enable		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: **0000000000000000000000000000000000000000**
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.

Regresar a la página de contenido

Regresar a la página de contenido

Descripción de iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- Funciones administrativas de iDRAC
- Características de seguridad de iDRAC
- Plataformas admitidas
- Sistemas operativos admitidos
- Exploradores web admitidos
- Conexiones de acceso remoto admitidas
- Puertos del iDRAC
- Otros documentos que puede necesitar

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 sistema de control y supervisión remotos. El iDRAC coexiste en la placa base con el servidor PowerEdge administrado. El sistema operativo del servidor, que puede ser un sistema operativo Microsoft® Windows® o Linux, se encarga de la ejecución de las aplicaciones; iDRAC se encarga de la supervisión y administración del estado y el entorno del servidor 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 M1000-e 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 pueden agregar CMC redundantes para estar protegido contra fallas en caso 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*. Las interfaces de red *dentro de banda* de los servidores administrados se pueden acceder a través de 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 de iDRAC

El iDRAC tiene las siguientes características de seguridad:

- Autentificación de usuarios por medio de Microsoft Active Directory (opcional) o mediante contraseñas e identificaciones de usuario almacenadas en el hardware
- Autoridad basada en funciones, la cual permite al administrador configurar 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, que admiten el cifrado SSL de 128 bits y el cifrado SSL de 40 bits (para países donde no se acepta el cifrado de 128 bits)
- Configuración del tiempo de espera de la sesión (en segundos) por medio de la interfaz web o SM-CLP
- Puertos de IP configurables (cuando sea aplicable)

  NOTA: Telnet no admite la codificación de 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 M1000-e:

- PowerEdge M600
- PowerEdge M605

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 compatibles con el iDRAC.

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 Web, Standard y Enterprise (x86 de 32 bits) con SP2 Microsoft Windows Server 2003 ediciones Standard y Enterprise (x64) con SP2 Microsoft Windows Storage Server 2003 R2 ediciones Express, Workgroup, Standard y Enterprise x64 Microsoft Windows Vista® ediciones Gold Business y Enterprise 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 el Service Pack 1, tenga presentes los cambios de la configuración de seguridad DCOM. Para obtener más información, consulte el artículo 903220 en el sitio web de asistencia de Microsoft en **support.microsoft.com/kb/903220**.
Red Hat® Linux®	Enterprise Linux WS, ES y AS (versión 3) (x86 y x86_64) 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

AVISO: La redirección de consola y los medios virtuales sólo admiten exploradores de web de 32 bits. La utilización de exploradores web de 64 bits producirá resultados inesperados o fallas.

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

Tabla 1-2. Exploradores web admitidos

Sistema operativo	Explorador web compatible
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 y Windows 2003 R2 SP2 solamente
Linux	Mozilla Firefox 1.5 (de 32 bits) en SUSE Linux (versión 10) solamente. Mozilla Firefox 2.0 (de 32 bits)

Conexiones de acceso remoto admitidas

La tabla 1-3 lista las características de las conexiones.

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 capturas SNMP y de correo electrónico • 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 iDRAC detecta las conexiones. La tabla 1-5 identifica los puertos que el iDRAC utiliza como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un iDRAC.

Tabla 1-4. Puertos de detección de servidor de iDRAC

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 de medios virtuales seguros
5900*	Redirección de teclado y mouse de consola
5901*	Redirección de vídeo de consola
* Puerto configurable	

Tabla 1-5. Puertos de cliente de iDRAC

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

Otros documentos que puede necesitar

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

- La ayuda en línea de iDRAC proporciona información sobre el uso de la interfaz web.
- La *Guía del usuario de Dell CMC con firmware versión 1.0* proporciona información sobre el uso del controlador que administra todos los módulos en el chasis que contiene el servidor PowerEdge.
- La *Guía del usuario de Dell OpenManage IT Assistant* y la *Guía de referencia de Dell OpenManage IT Assistant* proporcionan información sobre IT Assistant.
- La *Guía del usuario de Dell OpenManage Server Administrator* proporciona información sobre la instalación y el uso de Server Administrator.
- La *Guía del usuario de Dell Update Packages* ofrece información acerca de cómo obtener y utilizar 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* proporciona información importante de seguridad y normativas. La información de garantía se puede incluir en este documento o como documento independiente.
- La *Guía de instalación del estante* y las *Instrucciones de instalación en estante* que se incluyen con su solución de estante describen cómo instalar su sistema en un estante.
- La *Guía de introducción* proporciona una descripción general de las características del sistema, de cómo instalar el sistema y la especificaciones técnicas.
- El *Manual del propietario del hardware* proporciona información sobre las características del sistema y describe cómo solucionar los problemas del sistema y cómo instalar o sustituir los componentes del mismo.
- La documentación de Systems Management Software describe las características, requisitos, instalación y funcionamiento básico del software.
- La documentación del sistema operativo describe cómo instalar (si es necesario), configurar y utilizar el software del sistema operativo.
- La documentación de cualquier componente adquirido de forma independiente proporciona información para configurar e instalar estas opciones.
- A veces se incluyen actualizaciones con el sistema para describir cambios en el sistema, el software o la documentación.

  NOTA: Siempre lea primero las actualizaciones pues a menudo éstas reemplazan la información en otros documentos.

- Las notas de publicación o los archivos léame se pueden incluir para proporcionar actualizaciones de última hora del sistema así como documentación o material de referencia técnica avanzada pensado para usuarios con experiencia o técnicos.

Regresar a la página de contenido

Configuración del iDRAC

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- Antes de comenzar
- Interfaces para configurar el iDRAC
- Tareas de configuración
- Configuración del sistema de red por medio de la interfaz web del CMC
- Actualización del firmware del iDRAC

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 de Dell Chasis 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.

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

Tabla 2-1. Interfaces de configuración

Interfaz	Descripción
Utilidad de configuración del iDRAC	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 de 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 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 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: El cambio la configuración de la red de iDRAC termina todas las conexiones actuales de red del iDRAC.

NOTA: La opción para configurar el servidor que usa 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 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 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 filtros del sucesos de plataforma (PEF)
- RACADM: consulte Configuración del filtro de sucesos de plataforma

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

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 Configuración de la comunicación en serie en la LAN
- 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 Microsoft Windows o Linux 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 Reinicio automático de Windows

---

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

NOTA: Se deben tener privilegios de Administrador de configuración del chasis para definir la configuración de red de iDRAC desde el CMC.

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

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

1. Utilice el explorador web para iniciar sesión en la interfaz de usuario web del CMC si utiliza un 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 signo (+) que se encuentra junto a **Chasis** en la columna izquierda, luego haga clic en **Servidores**.
4. Haga clic en **Configuración**→ **Instalar**.
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 la IPMI en la LAN seleccionando o deseleccionando la casilla que se encuentra junto al servidor, bajo el encabezado **Activar IPMI en la 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 **Aplicar** en la parte inferior de la página.

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 mientras sino 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 Actualización del firmware del iDRAC por medio de SM-CLP.

Cuando utilice 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 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 Recuperación del firmware del iDRAC por medio del CMC.

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 utiliza 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 la salida generada. Esta opción se usa para actualizar el firmware sin conservar la información de configuración. Usted **no** debe utilizar 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

Una firma digital se usa para autentificar la identidad del firmante de un archivo y para certificar que el contenido original del archivo no ha sido modificado desde que fue firmado.

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 en la base de datos de confianza de GPG con el siguiente comando:

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

   NOTA: Usted debe tener la clave privada para completar el proceso.

3. Para evitar una advertencia de clave desconocida, cambie el nivel de confianza de la clave GPG pública de Dell.

   a. Escriba el comando siguiente:

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

   b. Dentro del editor de claves GPG, escriba `fpr`. Aparecerá el siguiente mensaje:

      ```
      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

      (pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Grupo de producto) <linux-security@dell.com>
      Huella digital de la clave principal: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951 23B6 6A9D)
      ```

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

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

      ```
      Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
      different sources, 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?

(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 = no sé o no diré
  2 = NO confío
  3 = confío en cierta medida
  4 = confío lo suficiente
  5 = confío plenamente
  m = volver al menú principal

¿Cuál es su decisión?)
```

d. Escriba 5 <Entrar>. Aparecerá la siguiente petición:

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

(¿Realmente desea otorgar plena confianza a esta clave? (S/N))
```

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

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

Usted 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, que 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 de Linux tiene el nombre **PE1850-BIOS-LX-A02.BIN**, el nombre del archivo de firma del mismo será **PE1850-BIOS-LX-A02.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 utilice 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 BIOS 1425SC:

1. Descargue los dos archivos siguientes de **support.dell.com**:
   - PESC1425-BIOS-LX-A01.bin.sign
   - PESC1425-BIOS-LX-A01.bin

2. Importe la clave pública ejecutando la línea de comandos siguiente:

   gpg --import <clave_pública_de_seguridad_de_linux.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

(gpg: clave 23B66A9D: "Dell Computer Corporation (Grupo de sistemas de Linux) <linux-security@dell.com>" sin cambios
gpg: número total procesado: 1
gpg: sin cambios: 1)
```

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

   a. Escriba el comando siguiente:

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

   b. En la petición de comandos, escriba el comando siguiente:

```
fpr
trust
```

   c. Escriba 5 <Entrar> para elegir I trust ultimately 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 PESC1425 por medio de la ejecución del comando siguiente:

```
gpg --verify PESC1425-BIOS-LX-A01.bin.sign PESC1425-BIOS-LX-A01.bin
```

Aparecerá el siguiente mensaje de salida:

```
gpg: Signature made Thu 14 Apr 2005 04:25:37 AM IST using DSA key ID 23B66A9D
gpg: Good signature from "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>"

(gpg: Firma realizada el jue 14 de abril de 2005 a las 04:25:37 IST con la ID de clave de DSA 23B66A9D
gpg: firma válida de "Dell Computer Corporation (Grupo de sistemas de Linux) <linux-security@dell.com>")
```

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

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D

(gpg: ADVERTENCIA: Esta clave no está certificada con una firma de confianza.
gpg: No hay ninguna indicación de que la firma pertenece al propietario.
Huella digital de la clave principal: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951 23B6 6A9D)
```

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 con firmware versión 1.00

- Pasos de configuración de la estación de administración
- Requisitos de la red de la estación de administración
- Configuración de un explorador web admitido
- Instalación de Java Runtime Environment (JRE)
- Instalación de clientes Telnet o SSH
- Instalación de un servidor TFTP
- Instalación de Dell OpenManage IT Assistant

Una estación de administración es un equipo que se utiliza 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 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 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 web admitidos, consulte Exploradores web admitidos.

NOTA: La interfaz web de iDRAC no se admite en exploradores web de 64 bits. Si abre un explorador web de 64 bits, accede a la página Redirección de consola e intenta instalar el complemento, el procedimiento de instalación fallará. Si este error no fuera reconocido y usted repite este procedimiento, la página Redirección de consola se cargará aunque la instalación del complemento falle en el primer intento. Este problema ocurre porque el explorador web almacena la información del complemento en el directorio del perfil, aunque haya fallado el procedimiento de instalación del complemento. Para resolver este problema, instale y ejecute un explorador web de 32 bits admitido e inicie sesión en iDRAC.

Configuración del explorador web para conectarse a la interfaz web

Si se conecta a la interfaz web de 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 de explorador web.
2. Haga clic en **Herramientas** y luego 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 está seleccionada la casilla **Usar servidor proxy**, seleccione la casilla **No usar servidor proxy para direcciones locales**.
6. Haga clic en **Aceptar** dos veces.

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 está 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
- Francés
- Alemán
- Español
- Japonés
- Chino simplificado

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 **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 su idioma preferido y haga clic en **Subir** para subir el idioma al inicio de la lista.
6. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.
7. Haga clic en **Aceptar**.

Firefox 1.5 (Linux)

Para ver una versión traducida de la interfaz web de iDRAC en Firefox, 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 **Aceptar**.

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

```
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 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="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 e inicie sesión en el sistema operativo.

Cuando cambie de cualquier otro idioma, compruebe este ajuste sigue siendo válido. De lo contrario, repita el 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 web Firefox.
2. En el campo de dirección, escriba `about:config` y presione <Entrar>:
3. En la columna **Nombre de preferencia**, encuentre y haga clic en **xpinstall.whitelist.required**.

   Los valores de **Nombre de preferencia**, **Estado**, **Tipo** y **Valor** cambiarán a texto en negritas. El valor de **Estado** cambiará a **definido por el usuario** y el parámetro **Valor** cambiará a **falso**.
4. En la columna **Nombre de preferencias**, localice **xpinstall.enabled**.

   Compruebe que **Valor** sea **true**. Si no es así, haga doble clic en **xpinstall.enabled** para definir **Valor** como **true**.

Instalación de Java Runtime Environment (JRE)

NOTA: Si utiliza 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. Consulte Configuración de la redirección de consola en la interfaz web del iDRAC para obtener más información.

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

Si utiliza 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.

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 824810 del sitio web de asistencia de Microsoft en **support.microsoft.com**. Para obtener más información, consulte el artículo 824810 de Microsoft Knowledge Base.

Configuración de la tecla de retroceso para la sesión telnet

Dependiendo del cliente telnet, al presionar la tecla <Retroceso> puede obtener resultados inesperados. Por ejemplo, la sesión puede mostrar ^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 tiene una sesión telnet abierta, escriba:

   ```
   telnet
   ```

   Si ya tiene una sesión telnet abierta, presione <Ctrl><]>.
3. En la petición, escriba:

   ```
   set bsasdel
   ```

   Aparecerá el siguiente mensaje:

   ```
   Backspace will be sent as delete.
   (La tecla de retroceso se enviará como "suprimir".)
   ```

Para configurar una sesión telnet de Linux para que pueda usar la tecla <Retroceso>, realice los pasos a continuación:

1. Abra una petición de comandos y escriba:

   ```
   stty erase ^h
   ```
2. En la petición, 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) o 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 ANSI o VT100 en Windows. La ejecución de OpenSSH en la petición de comandos de Windows no producirá una funcionalidad total (es decir, algunas teclas no responderán y no se mostrarán gráficos).

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

La implementación de SSH de iDRAC es compatible con varios esquemas de cifrado, según se muestra en la tabla 3-1.

NOTA: No se admite el SSHv1.

Tabla 3-1. Esquemas de cifrado

Tipo de esquema	Esquema
Criptografía asimétrica	De 512 a 1024 (aleatoriamente) bits de DSA/DSS de Diffie-Hellman de acuerdo a la especificación NIST
Criptografía simétrica	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Integridad del mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autentificación	• Contraseña

Instalación de un servidor TFTP

NOTA: Si utiliza 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 utiliza Linux, instale un servidor TFTP a partir de su distribución
- Si utiliza 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 componentes a continuación:

- 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 con firmware versión 1.00

- Instalación del software en el servidor administrado
- Configuración del servidor administrado para capturar la pantalla de último bloqueo
- Desactivación de la opción Reinicio automático de Windows

Esta sección describe 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 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 para crear secuencias de comando con tareas de configuración y administración.
- 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 estándares en 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. Usted puede ver los registros en la página de inicio, imprimirlos o guardarlos como informes y enviarlos por correo electrónico a un contacto designado de servicio.

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 Desactivación de la opción 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 de sistema automática.

   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 comando siguiente:

   ```
   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 ver 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 Reinicio automático de Windows

Para asegurar 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 **Avanzado**.
3. En **Inicio y recuperación**, haga clic en **Configuración**.
4. Deseleccione la casilla de marcación **Reiniciar automáticamente**.
5. Haga clic en **Aceptar** dos veces.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de iDRAC por medio de la interfaz web

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- Acceso a la interfaz web
- Configuración del NIC del iDRAC
- Configuración de sucesos de plataforma
- Configuración de IPMI
- Cómo agregar y configurar usuarios de iDRAC
- Cómo asegurar las comunicaciones de iDRAC por medio de certificados SSL y digitales
- Configuración y administración de los certificados de Active Directory
- Configuración de la comunicación en serie en la LAN
- Configuración de los servicios de iDRAC
- Actualización del firmware del iDRAC

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, utilice 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 acerca de 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 acerca de 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 de un explorador compatible web.

   Consulte Exploradores web admitidos para obtener más información.

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

   Si se ha cambiado el número predeterminado del 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 de iDRAC o como usuario de Microsoft® Active Directory®. El nombre de usuario y la contraseña predeterminados 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_it` 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. En las contraseñas se distingue entre mayúsculas y minúsculas.

3. Haga clic en **Aceptar** o pulse <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 sino hasta que usted haya iniciado sesión.

NOTA: El cierre del explorador sin una desconexión 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.

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 la red y los valores de la LAN de IPMI

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

NOTA: La mayoría de los servidores DHCP requieren que un servidor almacene un símbolo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este símbolo durante la negociación de DHCP. El 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 la red** y la **Configuración de la LAN 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 la tabla 5-3.

Tabla 5-1. Configuración de la red

Valor	Descripción
Activar el 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 del NIC)	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	Utiliza la dirección IP del servidor DNS secundario solamente cuando **no está seleccionada** la opción **Usar DHCP para obtener las direcciones del servidor DNS**. 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 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 de marcación **Usar DHCP para el nombre del dominio DNS**, seleccione también la casilla de marcación **Usar DHCP (para la dirección IP del 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 utilizar 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 de nivel de privilegio 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:** Al cambiar 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 utilizando la configuración actualizada de la dirección IP. Todos los demás cambios requerirán que se restablezca el NIC, lo que puede ocasionar una breve pérdida de la 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 la tabla 5-5.

Tabla 5-4. Configuración de la página de seguridad

Configuración	Descripción
Rango 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 de rango IP	Determina la dirección aceptable de subred IP. El valor predeterminado es **192.168.1.0**.
Máscara de subred de	Define las posiciones de bits significativos en la dirección IP. La máscara de subred debe darse en forma de máscara de red,

rango IP	donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior. El valor predeterminado es **255.255.255.0**.
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, la cual limita el número de intentos de inicio de sesión fallidos provenientes de una dirección IP específica dentro de un período previamente seleccionado. El valor predeterminado es **apagado**.
Número de fallos de bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión que se hicieron desde una dirección IP antes de que se rechacen los intentos de inicio de sesión provenientes de esa dirección. El valor predeterminado es **10**.
Ventana de fallos de bloqueo de IP	Determina el período en segundos dentro de cual deben ocurrir los incrementos al número de fallas para bloqueo de IP a fin de dar inicio al 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

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 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.

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 fue configurado para realizar una acción (por ejemplo, un reinicio del sistema), ésta se ejecutará.

Configuración de filtros del suceso de plataforma (PEF)

NOTA: Configure los filtros de sucesos de plataforma antes definir la configuración de alertas de captura de sucesos de plataforma o de correo electrónico.

1. Inicie sesión en la interfaz web del iDRAC. Consulte 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 dicho 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 debe estar activado para que las alertas se puedan enviar a un destino configurado válido (PET o correo electrónico).

Configuración de capturas de suceso de plataforma (PET)

NOTA: Debe contar con 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 web admitido. Consulte Acceso a la interfaz web.

2. Compruebe que siguió los procedimientos descritos en Configuración de filtros del suceso de plataforma (PEF).

3. Configure la dirección IP de destino de la captura de sucesos de plataforma:

   a. Haga clic en la casilla de marcación **Activar** junto al **Número de destino** que desee activar.

   b. Introduzca una dirección IP en la casilla **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 utilizar 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 las alertas de correo electrónico

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

2. Compruebe que siguió los procedimientos descritos en Configuración de filtros del suceso de plataforma (PEF).

3. Defina la configuración de la alerta de correo electrónico.

   a. En la ficha **Administración de alertas**, haga clic en **Configuración de la alerta por correo electrónico**.

4. Configure el destino de la alerta de 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 los pasos de la a a la 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 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** bajo **Configuración de la LAN de IPMI**, seleccione **Activar IPMI en la LAN**.

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

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz de IPMI en la LAN. Para obtener más información, consulte las especificaciones de 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. Defina la clave de cifrado 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 comunicación en serie en la LAN 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** y 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 es configurable.

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

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

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

   La tabla 5-8 describe los **Privilegios de 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 del **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 la 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 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 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 la **/** (diagonal) ni el **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el próximo inicio de sesión del mismo.
Cambiar contraseña	Activa los campos **Contraseña nueva** y **Confirmar contraseña nueva**. Cuando no está seleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Activa la edición de la contraseña del usuario de iDRAC. Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán.
Confirmar contraseña nueva	Vuelva a escribir la contraseña del usuario del iDRAC para confirmar.

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 utilizar la comunicación en serie en la LAN de IPMI. Cuando está seleccionada, este privilegio está activado.

Tabla 5-9. Privilegios de 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	Permite al usuario determinar los usuarios específicos que tendrán acceso al sistema.
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 la 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 (mensajes de correo electrónico y capturas de sucesos de plataforma) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Tabla 5-10. Permisos de grupo de 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 usuarios

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 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 un 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 candidato cumple los estándares de seguridad de la CA, ésta 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.

Cómo acceder al menú principal de SSL

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y 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 que están 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 sobrescribirá la CSR anterior en el firmware. Para que una CA acepte su CSR, la CSR del firmware debe coincidir con el certificado devuelto por la CA.
Cargar certificado del 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 X509, de base 64. No acepta certificados codificados DER.
Ver certificado del 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**.
Siguiente	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 la tabla 5-15.

Tabla 5-14. Opciones de la página de generación de solicitud de firma de certificados (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 de organización	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, Monterrey). Sólo son válidos los caracteres alfanuméricos y 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 espacios. No utilice abreviaturas.
Código de país	El nombre del país donde se ubica 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 de generación de solicitud de firma de certificados (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 del servidor

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

   Aparecerá la página **Carga del 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 de **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, lo cual incluye la ruta de acceso completa, el nombre de archivo completo y la extensión del archivo.

3. Haga clic en **Aplicar**.

4. Para continuar, haga clic en el botón correspondiente. Consulte la 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**.

Visualización de un certificado del 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 y las descripciones asociadas que aparecen en la ventana **Certificado**.

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

Tabla 5-17. Información del certificado

Campo	Descripción
Número de serie	Número serie del certificado
Información del titular	Atributos del certificado introducidos por el asunto
Información del emisor	Atributos del certificado devueltos por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de caducidad 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 los 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** y 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 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 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**.
Siguiente	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 los valores.
4. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 5-22.
5. Para configurar los grupos de funciones de Active Directory de esquema estándar, haga clic en el grupo de funciones individual (1-5). Consulte la tabla 5-23 y la 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
Habilitar Active Directory	Cuando está seleccionado, activa Active Directory. El valor predeterminado es **desactivado**.
Nombre del dominio raíz	El nombre del 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 esquema	Usa el esquema estándar con Active Directory.

estándar	
Usar 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 funciones, 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 del 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 la 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 de **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, lo cual incluye la ruta de acceso completa, el nombre de archivo completo y la extensión 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 la 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 pagina **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 y las descripciones asociadas enumeradas en la ventana **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 5-27.

Tabla 5-26. Información del certificado de CA de Active Directory

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

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 proporciona información sobre los valores de la página **Configuración de la comunicación en serie en la LAN**.
3. Haga clic en **Aplicar**.
4. Si es necesario, defina la configuración avanzada. De lo contrario, haga clic en el botón correspondiente para continuar. Consulte la 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. Consulte la tabla 5-30.

   c. Haga clic en **Aplicar**.

   d. Para continuar, haga clic en el botón correspondiente. Consulte la 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: Debe contar con permiso para **Configurar el iDRAC** para modificar estos valores.

NOTA: Cuando se aplican cambios en los servicios, los cambios surtirán efecto inmediatamente. Las conexiones existentes pueden ser terminadas sin advertencia.

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y 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 la configuración del servidor web
   - SSH: consulte la tabla 5-33 para la configuración de SSH
   - Telnet: consulte la tabla 5-34 para la configuración de Telnet
   - Agente de recuperación automatizada del sistema: consulte la tabla 5-35 para la configuración del agente de recuperación automatizada del sistema

4. Haga clic en **Aplicar**.

5. Para continuar, haga clic en el botón correspondiente. Consulte la 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**.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permiten para este sistema. Este campo no se puede editar. Pueden existir cuatro sesiones simultáneas.
Sesiones actuales	El número actual de sesiones en el sistema, menor o igual que el **N° máx. de sesiones**. Este campo no se puede editar.
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. Cuando se alcanza el tiempo de espera, la sesión se cancela. 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 segundos. El valor predeterminado es de **300** segundos.
Número de puerto HTTP	El puerto en el que el iDRAC espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto 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 SSH. Cuando está seleccionada, la casilla indica que SSH está activado.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permiten 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 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 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.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permiten 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 segundos. 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. Valor del agente de recuperación automatizada de sistemas

Valor	Descripción
Activado	Activa el agente de recuperación automatizada de sistemas.

Tabla 5-36. Botones de la página de 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 podría ocurrir si el progreso de actualización del firmware del iDRAC se interrumpe antes de terminar, usted puede recuperar el iDRAC por medio del CMC. Consulte la *Guía del usuario del firmware del CMC* para obtener instrucciones.

NOTA: La actualización del firmware, de manera predeterminada, retendrá los valores actuales 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** y después 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 a 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. Esto puede tardar varios minutos en concluir.

     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.
6. 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, medido 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 utilizando una ventana del explorador nueva.

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, la interfaz de línea de comandos del SM-CLP 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 sesión en la interfaz web del CMC.
3. Haga clic en **Chasis en el árbol del sistema**.
4. Haga clic en la ficha **Actualizar**. Aparecerá la página **Componentes que se pueden actualizar**. 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 con firmware versión 1.00

- Ventajas y desventajas del esquema ampliado y el esquema estándar
- Descripción de Active Directory de esquema ampliado
- Descripción del esquema estándar de Active Directory
- Habilitación de SSL en un controlador de dominio
- Uso de Active Directory para iniciar sesión en el iDRAC
- Preguntas frecuentes

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 el 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 dentro de 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 ninguna extensión de esquema, porque el esquema estándar usa únicamente los objetos de Active Directory.
- La configuración de Active Directory es sencilla.

Descripción de Active Directory de esquema ampliado

Hay tres maneras de activar Active Directory con el esquema ampliado:

- Con la interfaz web del iDRAC. Consulte Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web.
- Con la herramienta CLI de RACADM. Consulte Configuración del iDRAC con Active Directory de esquema ampliado por medio de RACADM.
- Con la línea de comandos de SM-CLP. Consulte Configuración del iDRAC con Active Directory de esquema ampliado y SM-CLP.

Ampliaciones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario pueden incluir el nombre, apellido, número de teléfono del usuario, etcétera. Las empresas pueden ampliar la base de datos de Active Directory agregando sus propios atributos y clases únicos para atender a las 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 se agrega a un esquema existente de Active Directory se debe definir con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de identificadores de objeto (OID) de Active Directory de modo que cuando las empresas agregan extensiones al esquema, pueden tener la garantía de que son únicas y que no tendrán conflictos entre sí. 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
Identificación de objeto base de Dell	1.2.840.113556.1.8000.1280
Rango de LinkID del RAC	De 12070 a 12079

Descripción de las ampliaciones de esquema del RAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de los clientes, Dell proporciona un grupo de propiedades que el usuario puede configurar en función de los resultados deseados. Dell ha ampliado el esquema para incluir las 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 ofrece la máxima flexibilidad a un administrador para las distintas combinaciones de usuarios, privilegios y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción de objetos de Active Directory

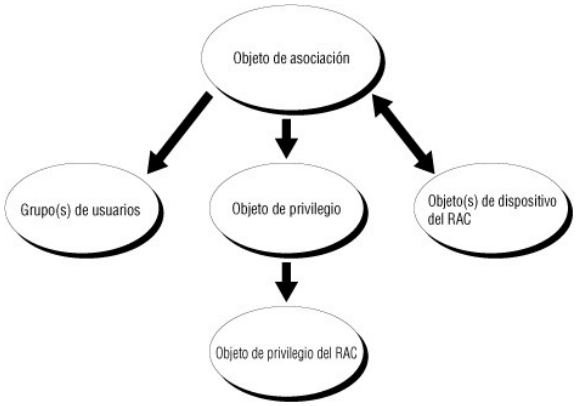
Para cada uno de los RAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de RAC. Puede crear varios objetos de asociación y cada uno de ellos se puede vincular a los usuarios, grupos de usuarios u objetos de dispositivo de RAC que se requiera. Los usuarios y los objetos de dispositivo de RAC pueden ser miembros de cualquier dominio en la empresa.

Sin embargo, cada objeto de asociación puede estar vinculado sólo a un objeto de privilegio (o bien, puede vincular usuarios, grupos de usuarios u objetos de dispositivo de RAC). Este ejemplo permite que un administrador controle los privilegios de cada usuario en 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 el objeto de dispositivo con el nombre de Active Directory de manera que los usuarios puedan llevar a cabo la autentificación y 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 ilustra que el objeto de asociación proporciona la conexión que es necesaria para toda la autentificación y autorización.

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.

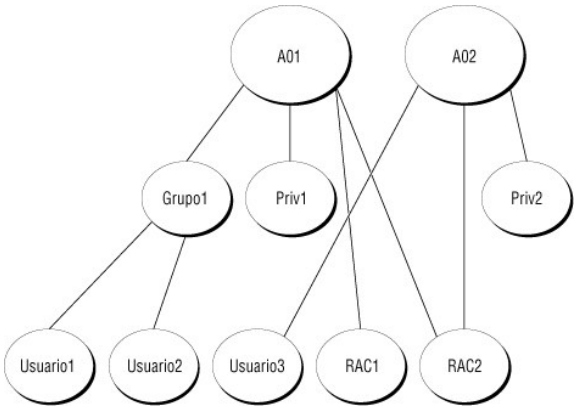
Usted puede crear la cantidad de objetos de asociación que necesite. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de RAC para cada RAC (iDRAC) en la red que desea integrar con Active Directory para fines de autentificación y autorización con el RAC (iDRAC).

El objeto de asociación tiene capacidad para cualquier cantidad de usuarios y/o grupos, así como de objetos de dispositivo de RAC. Sin embargo, el objeto de asociación incluye únicamente 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. La figura 6-2 le muestra cómo configurar los objetos de Active Directory en este escenario.

Cuando agregue grupos universales de dominios separados, cree un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados que son creados por la utilidad Dell Schema Extender son grupos locales del dominio y no funcionarán con los grupos universales de otros dominios.

Figura 6-2. Configuración de los objetos de Active Directory en un solo dominio



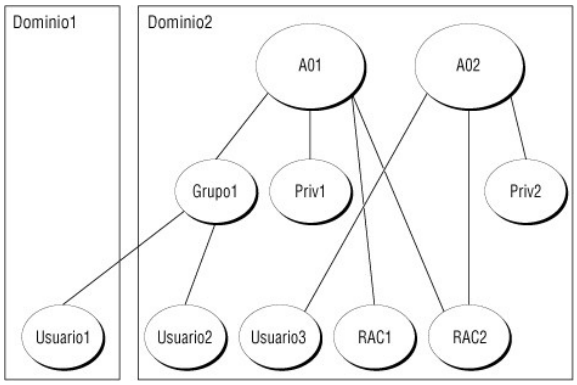
Para configurar los objetos para el escenario de un solo dominio, realice las siguientes tareas:

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 el Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
4. Agrupe usuario1 y usuario2 en el Grupo1.
5. Agregue a Grupo1 como miembro en el objeto de asociación 1 (AO1), Priv1 como objeto de privilegio en AO1, y RAC1, RAC2 como dispositivos RAC en AO1.
6. Agregue al usuario3 como miembro en el objeto de asociación 2 (AO2), Priv2 como objeto de privilegio en AO2, y RAC2 como dispositivos de RAC en AO2.

Consulte Cómo agregar usuarios y privilegios de iDRAC a Active Directory para ver instrucciones detalladas.

La figura 6-3 muestra un ejemplo de 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, y el usuario2 y el usuario3 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 los objetos de Active Directory en varios dominios



Para configurar los objetos para el escenario de varios dominios, realice las siguientes tareas:

1. Asegúrese que la función de bosque de dominio esté en los modos Nativo o Windows 2003.
2. Cree dos objetos de asociación, AO1 (de alcance universal) y AO2, 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 el Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
5. Agrupe usuario1 y usuario2 en el Grupo1. El alcance de grupo de Grupo1 debe ser universal.

6. Agregue a Grupo1 como miembro en el objeto de asociación 1 (AO1), Priv1 como objeto de privilegio en AO1, y RAC1, RAC2 como dispositivos RAC en AO1.

7. Agregue al usuario3 como miembro en el objeto de asociación 2 (AO2), Priv2 como objeto de privilegio en AO2, y RAC2 como dispositivos de RAC en AO2.

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 Ampliación del esquema de Active Directory).

2. Amplíe el complemento Usuarios y equipos de Active Directory (consulte Instalación de la extensión Dell en el complemento Usuarios y equipos de Active Directory).

3. Agregue los usuarios de iDRAC y sus privilegios en 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 Habilitación de SSL en un controlador de dominio).

5. Configure las propiedades de Active Directory de iDRAC utilizando la interfaz web de iDRAC o 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).

Ampliación del esquema de Active Directory

La ampliación del esquema de Active Directory agrega una unidad organizacional de Dell, clases y atributos de esquema y ejemplos de los objetos de privilegio y de asociación al esquema de Active Directory. Antes de ampliar el esquema, asegúrese de que tiene privilegios de Administrador de esquema en el propietario maestro de las funciones de operación maestra única flexible (FSMO) de esquema del bosque de dominio.

Puede ampliar su esquema usando una de las siguientes alternativas:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos de LDIF

Si usa el archivo de secuencia de comandos LDIF, la unidad organizativa 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 léame que se incluye en el directorio **LDIF_Files**. Para utilizar Dell Schema Extender para ampliar el esquema de Active Directory, consulte Uso de Dell Schema Extender.

Puede copiar y ejecutar Dell Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

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 **Bienvenido**, haga clic en **Siguiente**.

2. Lea detenidamente la advertencia y haga clic en **Siguiente**.

3. Seleccione **Usar las credenciales actuales de inicio de sesión** o introduzca un nombre de usuario y contraseña con derechos de administrador de esquema .

4. Haga clic en **Siguiente** para ejecutar el ampliador de esquemas de Dell.

5. Haga clic en **Terminar**.

   El esquema se ha ampliado. Para verificar la extensión de esquema, use la consola de administración de Microsoft (MMC) y el complemento de esquema de Active Directory para verificar que exista lo siguiente:

   - 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 clase	Número de identificación del 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 de RAC de Dell. El dispositivo de RAC debe ser 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
Súper clases	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
Súper clases	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
Súper clases	Ninguna
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	Se usa como clase de contenedor para los privilegios (derechos de autorización) de Dell.
Tipo de clase	Clase estructural

Súper clases	Usuario
Atributos	dellRAC4Privileges

Tabla 6-7. Clase dellProduct

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Descripción	La clase principal de la cual se derivan todos los productos Dell.
Tipo de clase	Clase estructural
Súper clases	Equipo
Atributos	dellAssociationMembers

Tabla 6-8. Lista de atributos agregados al esquema de Active Directory

Nombre/descripción del atributo	**OID asignada/sintaxis del identificador de objeto**	**Valor único**
dellPrivilegeMember Lista los objetos de dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellProductMembers Lista los objetos de dellRacDevices que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso de dellAssociationMembers. Identificación de vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellIsLoginUser Es "VERDADERO" si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsCardConfigAdmin Es "VERDADERO" si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsUserConfigAdmin Es "VERDADERO" si el usuario tiene derechos de configuración de usuarios en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
delIsLogClearAdmin Es "VERDADERO" si el usuario tiene derechos para borrar el registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsServerResetUser Es "VERDADERO" si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsConsoleRedirectUser Es "VERDADERO" 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)	VERDADERO
dellIsVirtualMediaUser Es "VERDADERO" si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsTestAlertUser Es "VERDADERO" si el usuario tiene derechos de prueba de alertas de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsDebugCommandAdmin Es "VERDADERO" si el usuario tiene derechos de administrador del comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellSchemaVersion Se usa la versión del esquema actual para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena para ignorar mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellRacType Este atributo es el tipo de RAC actual del 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 para ignorar mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSO

Lista los miembros dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo ligado de dellProductMembers. Identificación de vínculo: 12071	Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Instalación de la extensión Dell en el complemento 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 seleccionando la opción **Extensión de Dell al complemento Usuarios y equipos de Active Directory** durante el proceso de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para ver instrucciones adicionales de instalación del software Systems Management.

Para obtener más información acerca del complemento Usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Instalación del paquete de administrador

Debe instalar el paquete de administrador en cada sistema que administre los objetos de iDRAC de Active Directory. Si no instala el paquete de administrador, no podrá ver el objeto de RAC de Dell en el contenedor.

Consulte Apertura del complemento Usuarios y equipos de Active Directory para obtener más información.

Apertura del complemento Usuarios y equipos de Active Directory

Para abrir el complemento Usuarios y equipos de Active Directory, realice los pasos a continuación:

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

   Si no tiene una sesión abierta en el controlador de dominio, debe tener el paquete de administrador de Microsoft correspondiente instalado en su sistema local. Para instalar este paquete de administrador, haga clic en **Inicio**→ **Ejecutar**, escriba `MMC` y oprima **Entrar**.

   Aparecerá el servicio Microsoft Management Console (MMC).

2. En la ventana **Consola 1**, haga clic en **Archivo** (o **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 procedimientos siguientes:

- 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 consola** en MMC, haga clic con el botón derecho del mouse sobre un contenedor.

2. Seleccione **Nuevo**→ **Objeto de RAC de Dell**.

   Aparecerá la ventana **Nuevo objeto**.

3. Teclee un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC que escribió en el paso a de 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 **Aceptar**.

Creación de un objeto de privilegio

NOTA: Un objeto de privilegio se debe crear en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de la consola** (en MMC), haga clic con el botón derecho del mouse sobre un contenedor.
2. Seleccione **Nuevo→ Objeto de RAC de Dell**.

   Aparecerá la ventana **Nuevo objeto**.
3. Teclee un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **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 que el usuario tenga (para obtener más información, consulte Privilegios de usuario de iDRAC).

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El alcance de asociación especifica el tipo de grupo de seguridad del 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 se selecciona **Universal**, los objetos de asociación estarán disponibles únicamente cuando el dominio de Active Directory esté funcionando en modo nativo o superior.

1. En la ventana **Raíz de la consola** (en MMC), haga clic con el botón derecho del mouse sobre un contenedor.
2. Seleccione **Nuevo→ Objeto de RAC de Dell**.

   Esto abrirá la ventana **Nuevo objeto**.
3. Teclee un nombre para el nuevo objeto.
4. Seleccione **Objeto de asociación**.
5. Seleccione el alcance para el **Objeto de asociación**.
6. Haga clic en **Aceptar**.

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades del 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 su sistema ejecuta el modo Windows 2000 u otro superior, se deben usar grupos universales para extender los dominios con usuarios u objetos de RAC.

Usted puede agregar grupos usuarios y de dispositivos de RAC. El procedimiento para crear grupos relacionados de Dell y grupos no relacionados de Dell es idéntico.

Cómo agregar usuarios o grupos de usuarios

1. Haga clic con el botón derecho del mouse en **Objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de usuario o del grupo de 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 de usuario o de grupo de usuarios al autenticar un dispositivo de RAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

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

Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados a 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 **Productos** y haga clic en **Agregar**.
2. Escriba el nombre del dispositivo RAC o del grupo de dispositivos RAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y luego en **Aceptar**.

Configuración del iDRAC con Active Directory de esquema ampliado por medio de la interfaz web

1. Abra una ventana de un explorador compatible web.
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 Valores comunes:
   a. Seleccione la casilla de marcación **Habilitar Active Directory**.
   b. Escriba el **Nombre del dominio raíz**. El **Nombre del dominio raíz** es el nombre del dominio raíz completo del bosque.
   c. Escriba el valor de **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. Teclee el **Nombre de DRAC**. Este nombre debe ser el mismo que el nombre común del nuevo objeto de RAC que creó en el controlador de dominio (consulte el paso 3 de Creación de un objeto del dispositivo del RAC).
   b. Escriba el **Nombre del dominio de iDRAC** (por ejemplo, `iDRAC.com`). No use el nombre de NetBIOS. El **Nombre del dominio de DRAC** es el nombre del dominio completo del subdominio 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 al archivo del certificado o desplácese hasta el archivo del certificado.

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

    Los certificados SSL de los controladores de dominio deben tener la firma de la autoridad de certificados raíz. Tenga el certificado de CA raíz disponible en la estación de administración que 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 se selecciona **Usar DHCP (para la dirección IP del NIC)** en **Configuración de la red**, entonces seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

    Para introducir manualmente una dirección IP de servidor DNS, deseleccione **Usar el DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP primaria 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 ventana de símbolo del sistema y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

   racadm config -g cfgActiveDirectory -o 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_del_certificado_raíz_de_CA>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <URI_TFTP_del_certificado_de_servidor_del_iDRAC> /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_primaria_DNS>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_secundaria_DNS>
```

Descripción del esquema estándar de Active Directory

El uso del esquema estándar para la integración de Active Directory requiere la configuración de Active Directory y del iDRAC, según se muestra en la figura 6-4. En Active Directory, un objeto de grupo estándar se usa 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, el nivel de funciones y privilegios se define 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

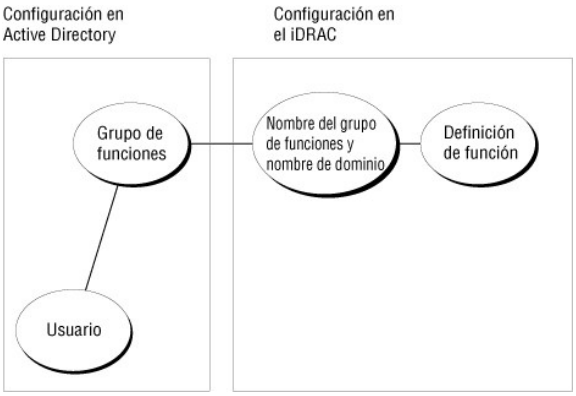


Tabla 6-9. Privilegios predeterminados del grupo de funciones

Nivel de privilegio predeterminado	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
Ninguna	Sin permisos asignados	0x00000000
Ninguna	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 Configuración del iDRAC con Active Directory de esquema estándar y la interfaz web.
- Con la herramienta CLI de RACADM CLI. Consulte 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 (controlador de dominio) Active Directory, abra el complemento de usuarios y equipos de Active Directory.
2. Cree un grupo o seleccione un grupo existente. El nombre del grupo y el nombre de este dominio deberán configurarse 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 de un explorador compatible web.
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 del **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 Valores comunes:
   a. Seleccione la casilla de marcación **Habilitar Active Directory**.
   b. Escriba el **Nombre del dominio raíz**. El **Nombre del dominio raíz** es el nombre del dominio raíz completo del bosque.
   c. Escriba el valor de **Tiempo de espera** en segundos.
7. Haga clic en **Usar esquema estándar** 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 **Grupo de funciones**.

   Aparecerá la página **Configurar grupo de funciones**, que incluye el **Nombre de grupo**, el **Dominio del grupo** y los **Privilegios del grupo de funciones** del grupo de funciones.
10. Teclee el **Nombre de grupo**. El nombre de grupo que identifica el grupo de funciones en Active Directory relacionado con el iDRAC.
11. Teclee el **Dominio del grupo**. El **Nombre del grupo** es el nombre del dominio raíz completo del 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 al archivo del certificado o desplácese hasta el archivo del certificado.

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

    Los certificados SSL de los controladores de dominio deben tener la firma de la autoridad de certificados raíz. Tenga el certificado de CA raíz disponible en la estación de administración que 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 después haga clic en **Red**.
20. Si se selecciona **Usar DHCP (para la dirección IP del NIC)** en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

    Para introducir manualmente una dirección IP de servidor DNS, deseleccione **Usar el DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP primaria 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 ventana de símbolo del sistema y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 2

   racadm config -g 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 conocer los valores de la 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 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, utilice 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_raíz_de_CA>

   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_primaria_de_DNS>

   set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
   dnsendpt1/remotesap1 dnsserveraddress=<dirección_IP_secundaria_de_DNS>
   ```

Habilitación 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 Entidad emisora raíz de la empresa de Microsoft 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 de marcación de **Servicios de certificado**.
   d. Seleccione **Entidad emisora raíz de la empresa** como **Tipo de entidad emisora de certificados** y haga clic en **Siguiente**.
   e. Escriba el **Nombre común para esta entidad emisora de certificados**, haga clic en **Siguiente** y haga clic en **Terminar**.

2. Active SSL en cada uno de los controladores de dominio instalando el certificado SSL para cada controlador.
   a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Directiva de seguridad de dominio**.
   b. Expanda la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse **Configuración de la petición de certificados automática** y haga clic en **Petición de certificados automática**.
   c. En **Asistente para instalación de petición automática de certificado**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y haga clic en **Terminar**.

Exportación del certificado de CA de raíz del controlador de dominio

NOTA: Si el sistema ejecuta Windows 2000, los pasos a continuación pueden variar.

1. Localice el controlador de dominio que ejecuta el servicio Microsoft Enterprise CA.
2. Haga clic en **Inicio**→ **Ejecutar**.
3. En el campo **Ejecutar**, escriba mmc y haga clic en **Aceptar**.

4. En la ventana **Console 1** (MMC), haga clic en **Archivo (**o **Consola** en los equipos 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 **Aceptar**.
10. En la ventana **Consola 1,** amplíe la carpeta **Certificados,** amplíe la carpeta **Personal**, y haga clic en la carpeta **Certificados**.
11. Ubique y haga clic con el botón derecho del mouse en el certificado de CA raíz, seleccione **Todas las tareas** y haga clic en **Exportar...**.
12. En el **Asistente para exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **X.509 codificado base 64 (.cer)** como formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio en el sistema.
15. Cargue el certificado que guardó en el paso 14 en el iDRAC.

    Para cargar el certificado usando 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 de un explorador compatible web.
    b. Inicie sesión en la interfaz web del iDRAC.
    c. Haga clic en **Sistema**→ **Acceso remoto** 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 del certificado de seguridad**, seleccione **Cargar certificado del servidor** y haga clic en **Aplicar**.
    f. En la pantalla **Carga del certificado**, realice uno de los procedimientos siguientes:
        - Haga clic en **Examinar** y seleccione el certificado.
        - En el campo **Valor**, escriba la ruta de acceso al 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 pasos a continuación 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 de dominio, abra una ventana de **Consola de MMC** y seleccione **Certificados**→ **Autoridades de certificación raíz de confianza**.
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 localice el archivo del certificado SSL.
4. Instale el certificado de SSL de RAC en la **Autoridad de certificados raíz de confianza** de cada controlador de dominio.

   Si ha instalado su propio certificado, compruebe que la autoridad de certificación que firma el certificado esté en la lista **Entidad emisora raíz de confianza**. Si la autoridad no está en la lista, deberá instalarla en todos los controladores de dominio.
5. Haga clic en **Siguiente** y seleccione si desea que Windows seleccione automáticamente al proveedor de certificados basándose en el tipo de certificado, o explore un proveedor de su preferencia.
6. Haga clic en **Terminar** y haga clic 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. Utilice uno de los formatos siguientes para introducir el nombre de usuario:

<nombre_de_usuario@dominio>

o

<dominio>\<nombre_de_usuario>

o

<dominio>/<nombre_de_usuario>

donde *nombre_de_usuario* es una cadena ASCII de 1 a 256 bytes.

No se pueden usar espacios en blanco ni caracteres especiales (como \, /, o @) en el nombre de usuario ni en el nombre del dominio.

NOTA: No pueden especificar nombres de dominio NetBIOS, como "América", porque no es posible establecer un vínculo con estos nombres.

Preguntas frecuentes

La tabla 6-10 muestra una lista de preguntas y respuestas frecuentes.

Tabla 6-10. Uso de iDRAC con Active Directory: Preguntas frecuentes

Pregunta	Respuesta
¿Puedo iniciar sesión en el iDRAC utilizando Active Directory entre varios árboles?	Sí. El algoritmo de consulta de Active Directory del iDRAC admite varios árboles en un solo bosque.
¿Funciona el inicio de sesión en el iDRAC por medio de Active Directory 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 utiliza (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 el objeto de asociación, los objetos de usuario del RAC y los objetos de dispositivo del 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 extendido de 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 SSL del controlador de dominio?	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 usted usa los servicios de certificados de Microsoft para generar el certificado del RAC, una causa probable de esto es que usted por descuido haya elegido **Certificado de usuario** en vez **Certificado de web** cuando creó 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_web_ssl}
¿Qué puedo hacer si no puedo iniciar sesión en el iDRAC mediante la autentificación de Active Directory? ¿Cómo soluciono el problema?	1. Asegúrese de que está usando el nombre del dominio de usuario correcto durante el inicio de sesión y no el nombre de NetBIOS. 2. Si tiene una cuenta de usuario local de iDRAC, inicie sesión en el iDRAC utilizando 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 de que el **Nombre del DRAC**, el **Nombre del dominio raíz** y el **Nombre del dominio de DRAC** coincidan con la configuración del 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

Uso de la redirección de consola con interfaz gráfica de usuario

Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- Descripción
- Uso de redirección de consola
- Uso de Video Viewer
- Preguntas frecuentes

Esta sección proporciona información acerca de cómo usar la función de redirección de consola de iDRAC.

Descripción

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 se puede utilizar junto con la característica 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.
- El ancho de banda de red mínima requerida es de 1 MB/seg.

Resoluciones de pantalla admitidas y frecuencias de actualización

La tabla 7-1 contiene una lista de las resoluciones de pantalla admitidas y de las frecuencias de actualización correspondientes, para una sesión de redirección de consola que se esté ejecutando en el servidor administrado.

Tabla 7-1. Resoluciones de pantalla admitidas y frecuencias de actualización

Resolución de pantalla	Frecuencia de actualización (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Configuración de la estación de administración

Para usar el redirección de consola en la estación de administración, realice los procedimientos siguientes:

1. Instale y configure un explorador web admitido. Consulte las secciones siguientes para obtener más información:
   - Exploradores web admitidos

   AVISO: La redirección de consola y los medios virtuales sólo admiten exploradores de web de 32 bits. La utilización de exploradores web de 64 bits puede generar resultados inesperados o falla de operaciones.

   - Configuración de un explorador web admitido

2. Si utiliza Firefox o desea usar el visor de Java con Internet Explorer, instale Java Runtime Environment (JRE). Consulte 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 7-2 describe los valores de la redirección de consola.

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

5. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 7-3.

Tabla 7-2. 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**.
N° máx. de sesiones	Muestra el número máximo posible de sesiones de redirección de consola, **1** ó **2**.Utilice 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 de puerto del 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 de puerto de vídeo	El número de puerto de red que se utiliza para conectar al servicio de pantalla de 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 utilice 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:** Deberá tener instalado Java Runtime Environment en el sistema cliente a fin de usar al 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 utilizando **Redirección de consola** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener información sobre cómo utilizar los medios virtuales con la redirección de consola, consulte Configuración y uso de medios virtuales.

Los botones de la tabla 7-5 están disponibles en la página **Configuración de la redirección de consola**.

Tabla 7-3. Botones de la página de configuración de la redirección de consola

Botón	Definición
Imprimir	Imprime la página **Configuración de la redirección de consola**
Actualizar	Vuelve a cargar 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 en la tabla 7-4 para asegurarse que haya una sesión de redirección de consola disponible.

   Si desea reconfigurar cualquiera de los valores de propiedad que se muestran, consulte Configuración de la redirección de consola en la interfaz web del iDRAC.

Tabla 7-4. Información de página de redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No
Cifrado de vídeo activado	Sí/No
N° 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 está seleccionado, los usuarios utilicen la conexión iKVM en el chasis no podrán acceder a la consola.

NOTA: Para obtener información sobre cómo utilizar los medios virtuales con la redirección de consola, consulte Configuración y uso de medios virtuales.

Los botones de la tabla 7-5 están disponibles en la página **Redirección de consola**.

Tabla 7-5. Botones de página de redirección de consola

Botón	Definición
Actualizar	Vuelve a cargar 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 múltiples casillas de mensaje después de iniciar la aplicación. Para prevenir el acceso no autorizado a la aplicación, se debe navegar a través de estos cuadros de mensajes en 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 de visor de KVM digital de Dell.

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 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 7-6 describe las opciones del menú que están disponibles en el visor.

Tabla 7-6. Selecciones de la barra de menú del visor

Opción 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. Se muestra un cuadro de diálogo que permite guardar el archivo en una ubicación especificada.
	Pantalla completa	Para expandir el Video Viewer al modo de pantalla completa, seleccione **Pantalla completa** desde el menú **Vídeo**.
	Salir	Cuando haya terminado de utilizar 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**.
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: • Control-Alt-Supr • Alt-Tab • Alt-Esc • Control-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 utilice 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 el componente de medios virtuales, consulte Configuración y uso de medios virtuales. Se debe mantener activa la ventana del visor de consola cuando se utilizan los medios virtuales.
Ayuda	N/A	Activa el menú **Ayuda**.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema PowerEdge remoto utilizando 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 utiliza 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* **N° 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 con el 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. Consulte Acceso a la interfaz web para obtener más información.
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 frecuentes

La tabla 7-7 muestra una lista de preguntas y respuestas frecuentes.

Tabla 7-7. 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, 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	Cualquier usuario con privilegios de configuración del iDRAC puede activar o desactivar la consola local.

del servidor local?	
¿Cómo puedo averiguar 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 de abajo de la pantalla del sistema en la ventana de la redirección de consola.	Compruebe que la resolución del monitor de la estación de administración sea 1280x1024.
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. Consulte Cómo establecer la configuración regional en Linux para obtener más información.
¿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 no se sincroniza el mouse en DOS al realizar una redirección de consola?	EL BIOS de Dell emula el archivo controlador del mouse como si fuera un mouse PS/2. Según su diseño, el mouse PS/2 usa la posición relativa para el apuntador del mouse, lo cual genera un retraso en la sincronización. El iDRAC tiene a un archivo controlador de mouse USB, lo que permite tener una 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 el mouse no se sincroniza en la consola de texto de Linux?	El KVM virtual requiere del archivo controlador de mouse USB, pero dicho archivo 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 alertar al usuario que la redirección de consola está activada. Para asegurarse de que este mensaje no aparezca, desactive siempre la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador Bloq Num de mi estación de administración no refleja el estado del Bloq Num 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 del indicador Bloq Num depende del valor que tenga el servidor remoto cuando la sesión remota está conectada, independientemente del estado del Bloq Num en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una sesión de redirección de consola desde el host local?	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, tendrán el control del sistema.
¿Cuánta amplitud de banda necesito para poder ejecutar una sesión de redirección de consola?	Dell recomienda una conexión de 5 MB/s para tener un buen rendimiento. Se requiere una conexión de 1 MB/s para tener el rendimiento mínimo.
¿Cuáles son los requisitos mínimos de sistema para que mi estación de administración pueda ejecutar 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

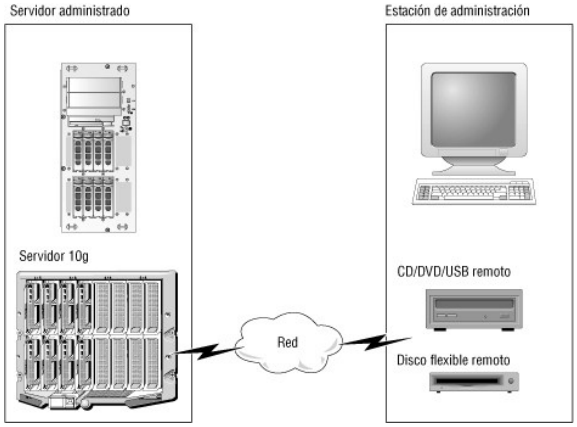
Guía del usuario de Integrated Dell™ Remote Access Controller con firmware versión 1.00

- Descripción
- Configuración de los medios virtuales
- Ejecución de los medios virtuales
- Preguntas frecuentes

Descripción

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 8-1 muestra la arquitectura general de los **Medios virtuales**.

Figura 8-1. Arquitectura general de los 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 en 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 8-1 muestra una lista de las conexiones de unidades admitidas para las unidades ópticas y de disco flexible virtuales.

NOTA: Cambiar **Medios virtuales** mientras está conectado podría detener la secuencia de inicio de sistema.

Tabla 8-1. Conexiones de unidades admitidas

Conexiones admitidas de unidades de disco flexible virtuales	Conexiones admitidas de unidades ópticas virtuales
Unidad heredada de disco flexible de 1,44 con un disco de 1,44 pulgadas	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disco flexible USB con un disco 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 con el complemento de control de ActiveX. Establezca la seguridad del explorador en **Medio** o otro nivel menor para permitir que Internet Explorer descargue e instale los controles firmados de ActiveX.

Consulte Exploradores web admitidos para obtener más información.

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 le muestre una 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. 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 iDRAC.
2. Seleccione **Sistema** en el árbol de navegación y haga clic en la ficha **Consola**.
3. Haga clic en **Configuración**→ **Medios virtuales** para definir la configuración de los medios virtuales.

   La tabla 8-2 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 la tabla 8-3.

Tabla 8-2. 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.
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 utiliza para conectarse al servicio de **Medios virtuales** sin cifrado. Dos puertos consecutivos a partir del número de puerto especificado se utilizan 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 utilizan 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 8-3. 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 ejecute 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 se esté accediendo a los medios virtuales.

1. Abra un explorador web admitido en la estación de administración. Consulte Exploradores web admitidos.

   AVISO: La redirección de consola y los **Medios virtuales** sólo admiten exploradores de web de 32 bits. El uso de exploradores web de 64 bits puede producir resultados inesperados o fallas.

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** en **Unidad de disco flexible** (si se aplica), pues este dispositivo puede ser tratado como disco virtual. Puede seleccionar una unidad óptica y un disco flexible al mismo tiempo, o bien, 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: Los **Medios virtuales** pueden no funcionar correctamente en clientes con sistema operativo Windows que estén configurados con seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo Microsoft o póngase en contacto con su 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 medio 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 **Cerrar**.

Inicio a partir de 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 están activadas y listadas 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 abrir la ventana de configuración del BIOS.

3. Desplácese hasta la secuencia de inicio y presione <Entrar>.

   En la ventana emergente, las unidades ópticas virtuales y de disquete se presentan en una lista con los dispositivos normales de inicio.

4. Asegúrese que la unidad virtual está activada y que aparece en la lista como el primer dispositivo con medios iniciables. De ser necesario, siga las instrucciones en la pantalla para modificar el orden de inicio.

5. Guarde los cambios y cierre.

   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 ignora el dispositivo, como en el caso de un dispositivo físico sin medios iniciables.

Instalación de sistemas operativos mediante los 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 para concluir. 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 del sistema operativo está insertado en la unidad de CD de la estación de administración.
   - La unidad local de CD está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar los medios virtuales indicados en la sección Inicio a partir de medios virtuales para asegurar que el BIOS esté configurado para iniciarse a partir de la unidad de CD desde la que se está realizando la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

Uso de los medios virtuales cuando el sistema operativo del servidor está funcionando

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 en el entorno 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 frecuentes

La tabla 8-4 muestra una lista de preguntas y respuestas frecuentes.

Tabla 8-4. 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 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 pierdo a veces mi conexión de cliente?	• Algunas veces, usted puede perder su conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si usted cambia el CD en la unidad de CD del sistema cliente, el nuevo CD podría tener una función de ejecución automática. Si es así, el firmware puede agotar el tiempo de espera y la conexión puede perderse si el sistema cliente también tarda mucho en estar listo para leer el CD. Si una conexión se pierde, vuelva a conectarse a partir de la interfaz gráfica de usuario y siga 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 tomar demasiado tiempo. ¿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. Aunque la ventana de instalación no muestra el progreso, el proceso de instalación está en progreso.
Veo el contenido de una unidad de disco virtual o de una clave de memoria USB. Si trato de establecer una conexión de medios virtuales usando la mismo unidad, recibo un mensaje de falla de conexión pidiéndome que lo intente de nuevo. ¿Por qué?	No se permite acceder simultáneamente a unidades de disco flexible virtuales. Cierre la aplicación utilizada para ver el contenido de la unidad antes de intentar virtualizar la unidad.
¿Cómo configuro el dispositivo virtual como un dispositivo iniciable?	En el servidor administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Encuentre el CD virtual, el disco flexible virtual o la unidad flash virtual y cambie el orden de inicio de dispositivos según sea necesario. Por ejemplo, para iniciar desde una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.
¿A partir de qué tipo de medios puedo iniciar?	El iDRAC permite iniciar a partir de los medios iniciables siguientes: • Medios de datos CDROM/DVD • Imagen ISO 9660 • Disco flexible 1.44 o imagen de disco flexible • Una clave USB reconocida por el sistema operativo como disco extraíble • Una imagen de clave USB
¿Cómo puedo hacer que mi clave 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 el símbolo del sistema 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 la 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 yo estoy conectado a un disco 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 semejante. 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 a continuación para encontrar y montar correctamente la unidad de disco flexible virtual: 1. Abra una línea de comandos de Linux y ejecute el comando siguiente: `grep "Virtual Floppy" /var/log/messages` 2. Localice la última entrada de ese mensaje y anote la hora. 3. En el símbolo del sistema Linux, ejecute el comando siguiente: `grep "hh:mm:ss" /var/log/messages` donde: *hh:mm:ss* es la hora del mensaje generado por grep 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. Compruebe que no esté adjuntado y conectado a la unidad de disco virtual. 6. En el símbolo del sistema de Linux, ejecute el comando siguiente: `mount /dev/sdx /mnt/floppy` donde: */dev/sdx* es el nombre del dispositivo encontrado 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 con firmware versión 1.00

- Uso del comando RACADM
- Subcomandos de RACADM
- Uso de la utilidad RACADM para configurar el iDRAC
- Uso de un archivo de configuración de iDRAC
- Configuración de varios iDRAC

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 las información siguiente:

- 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

La tabla 9-1 proporciona una descripción de cada subcomando de RACADM que usted puede ejecutar en RACADM. Para ver una lista detallada de los subcomandos de RACADM, incluso la sintaxis y las anotaciones válidas, consulte Descripción de subcomandos de RACADM.

Tabla 9-1. 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, incluso 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 información sobre el 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 CA o un certificado de servidor en el iDRAC.
sslcertview	Muestra un certificado CA o un certificado de servidor en el iDRAC.
sslcsrgen	Genera y descarga la CSR de la 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.
vmdisconnect	Obliga a una conexión de medios virtuales a cerrarse.

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 descripciones completas 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. Se perderán todos los cambios anteriores.

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 ser activados y desactivados con el transcurso del tiempo. 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 dieciseisavo usuario está reservado para el usuario de la LAN de IPMI.) Antes de habilitar manualmente a un usuario de iDRAC, verifique si hay 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. 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. Configure el privilegio de inicio de sesión en el iDRAC para el usuario.
4. Habilite al 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 la tabla 9-2:

Tabla 9-2. Máscaras de bit para privilegios del usuario

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

Por ejemplo, para otorgar privilegios de **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros** y **Acceder a la redirección de consola** al usuario, agregue los 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

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

El ejemplo a continuación muestra la sintaxis de comando que se puede usar para eliminar un usuario del RAC:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <indice> ""
```

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. Consulte Configuración de las alertas de correo electrónico para obtener más información.

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 envío de alertas de capturas SNMP del iDRAC, asegúrese que los valores de SNMP y de las capturas 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 de red disponibles, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Para usar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** y activar esta función:

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

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración de iDRAC cuando se le pide que teclee <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 de IPMI en la LAN. Para obtener más información, consulte las especificaciones de 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 establecer el privilegio de canal de LAN de IPMI como 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+. Para obtener más información, consulte las especificaciones de IPMI 2.0.

```
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 privilegio mínimo de SOL de IPMI determina el privilegio mínimo que se necesita para activar la comunicación en serie en la LAN de IPMI. Para obtener más información, consulte la especificación de 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 valores:

- 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 serie en la LAN, asegúrese que la velocidad en baudios de SOL sea idéntica a la velocidad en baudios del servidor 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 ó 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: La comunicación en serie en la LAN puede activarse o desactivarse individualmente para cada usuario.

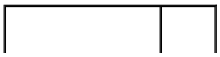
```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <identificación> 2
```

donde *<identificación>* es la identificación exclusiva del usuario.

Configuración del filtro de sucesos de plataforma

Puede configurar la acción que desea que el iDRAC ejecute ante cada alerta de plataforma. La tabla 9-3 muestra las acciones posibles y el valor para identificarlas en RACADM.

Tabla 9-3. 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 del filtro de sucesos de plataforma (consulte la tabla 5-6) y <*valor_de_la_acción*> es un valor de la tabla 9-3.

   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` ó `1` desactiva o activa la captura de sucesos de plataforma, respectivamente.

   Por ejemplo, para activar la captura de sucesos de plataforma con el 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 la petición 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 las alertas de 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 del destino del mensaje de correo electrónico puede ser un valor de 1 a 4.

   Por ejemplo, para activar el correo electrónico con el 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.

La filtración 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 **cfgRacTuning**:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propiedad **cfgRacTuneIpRangeMask** se aplica tanto a la propiedad de la dirección IP entrante como a la propiedades **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 las direcciones IP que estén fuera de este rango recibirán un mensaje de error.

Si la expresión siguiente es igual a cero, se procederá con el inicio de sesión:

```
cfgRacTuneIpRangeMask & (<dirección_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

donde & es el modo en bits "AND" de las cantidades y ^ es el modo en bits exclusivo "OR".

Consulte cfgRacTuning para ver una lista completa de las propiedades de **cfgRacTuning**.

Tabla 9-4. Propiedades de filtración de direcciones IP (IpRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación del rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de direcciones IP aceptable, según los unos (1) que haya en 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 de bits significativos 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 de 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 comandos de RACADM.

1. Los siguientes comandos de RACADM bloquean todas las direcciones IP excepto la 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 todos los bits, excepto los dos últimos en la máscara, como 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 de filtración de IP

Siga las siguientes directrices al momento de activar la filtración de IP:

- Asegúrese que **cfgRacTuneIpRangeMask** esté configurada en forma de máscara de red, donde todos bits más significativos son unos (1) (lo que define la subred en la máscara) con una transición total a ceros (0) en los bits del orden 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 del orden inferior en donde la máscara tiene ceros.

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 fallas 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 SSH pueden mostrar el mensaje siguiente: identificación de intercambio de SSH: El host remoto cerró 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 **cfgRacTune**.

Las Propiedades de restricción de reintento de inicio de sesión muestra los parámetros definidos por el usuario.

Tabla 9-5. 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 dirección IP determinada 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 permitido de fallas de inicio de sesión provenientes de una dirección IP antes de comenzar a rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El periodo en segundos durante el cual se cuentan los intentos fallidos. Cuando las fallas superan este límite, se quitan 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 impide que se realicen más de tres intentos fallidos dentro de un minuto e impide más intentos de inicio de sesión 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 <nuevo número de 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 puede ser:

- Creado con un editor de textos
- Obtenido del iDRAC con el subcomando **getconfig** de RACADM
- Obtenido 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:

  ```
  #

  # This is a comment (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 cualquier objeto en dicho grupo. Los objetos que no incluyan un nombre de grupo asociado generarán un error. La información de configuración está organizada en grupos, como se define en Definiciones de grupos y objetos de la base de datos de propiedades de iDRAC.

  El ejemplo siguiente muestra un nombre de grupo, objeto y el valor de la 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 se deja sin modificación. 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.

  Usted *no puede* especificar el índice que se utiliza. Si el índice ya existe, se está usando, o bien, la nueva anotación se crea en el primer índice disponible para ese 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: Puede crear un grupo indexado manualmente con el comando siguiente:
racadm config -g <*Nombre_de_grupo*> -o <*objeto_anclado*> -i <*índice*> <*nombre_único_de_ancla*>

- La línea para un grupo indexado *no se puede borrar* de un archivo de configuración.

  Usted debe quitar un objeto indexado manualmente por medio del siguiente comando:

  ```
  racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> -i <índice> ""
  ```

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 comando siguiente:

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

- Para grupos indexados, el ancla de objeto *debe ser* el primer objeto después del par *[ ]*. A continuación, se presentan ejemplos de los grupos indexados actuales:

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<nombre_de_usuario>
  ```

- Si el analizador encuentra un grupo indexado, el valor del objeto delimitado será el que distinga entre 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 borrar, de manera que con el tiempo, es posible que el grupo se vaya fragmentando con índices usados y sin usar. Si hay un índice presente, éste se modifica. Si no hay un índice presente, se usará el primer índice disponible. Este método ofrece flexibilidad al momento de agregar anotaciones indexadas en las que usted no tiene que hacer coincidencias exactas de índice entre todos los RAC que se están administrando. Los nuevos usuarios se agregan 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 innecesarias de **<***variable***>**=<*valor*>. Sólo la etiqueta variable real del grupo con "[" y "]" permanecerá, incluyendo las dos anotaciones **<***variable***>**=<*valor*> correspondientes al cambio de la dirección IP.

Por ejemplo:

```
#

# Object Group (Grupo de objetos) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo se actualizará como se muestra a continuación:

```
#

# Object Group (Grupo de objetos) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (comentario, el resto de esta línea se ignora)

cfgNicGateway=10.35.9.1
```

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 observen 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 raíz está disponible, la configuración de los demás usuarios también se restablece en sus valores predeterminados.

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 reproducir 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**.

   Consulte Creación de un archivo de configuración de iDRAC para obtener más información.

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 creó 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 creó. 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 con firmware versión 1.00

- Administración del sistema con SM-CLP
- Compatibilidad con SM-CLP de iDRAC
- Características de SM-CLP
- Navegación del espacio de direcciones del punto de acceso de administrabilidad
- Uso del verbo show
- Ejemplos de SM-CLP del iDRAC
- Uso de la comunicación en serie en la LAN (SOL) con Telnet o SSH

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: En esta sección se asume que usted está familiarizado con la iniciativa de la arquitectura de administración de sistemas para hardware de servidor (SMASH) y con las especificaciones SM-CLP de SMWG. Para más información sobre estas especificaciones, consulte el sitio web de la Distributed Management Task Force (DMTF), 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 lograr el objetivo de tener una arquitectura SMASH definida que constituya los cimientos 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 que el DMTF está impulsando.

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 y 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 conocer la correlación entre los comandos de RACADM y los de SM-CLP.

Administración del sistema con SM-CLP

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: encender, apagar o reiniciar el sistema
- Administración del registro de sucesos del sistema (SEL): muestra o borra las anotaciones del SEL
- 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 secciones siguientes proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC.

Características 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>]
```

La tabla 10-1 muestra una lista de los verbos compatibles con la CLI del iDRAC, la sintaxis de cada comando y una lista de las opciones de verbos que son compatibles.

Tabla 10-1. 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 la instancia de 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 del 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 los subdestinos, las propiedades y los verbos 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	Apaga 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

La tabla 10-2 describe las opciones de SM-CLP. Algunas opciones tienen formas abreviadas, según se muestra en la tabla.

Tabla 10-2. Opciones admitidas de SM-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 del punto de acceso de administrabilidad

NOTA: La diagonal (/) y la diagonal invertida (\) son intercambiables 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 principal y `.` se refiere al nivel actual.

Destinos

La tabla 10-3 muestra una lista de destinos disponibles por medio de SM-CLP.

Tabla 10-3. Destinos de SM-CLP

Destino	Definición
/system1/	El sistema administrado de destino.
/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 de usuario local del 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 instancia individual de anotación del SEL 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**, las cuales 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 SEL
- Navegación del punto de acceso de administrabilidad 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

Administración de la alimentación del servidor

La tabla 10-4 muestra ejemplos de cómo usar el SM-CLP para realizar operaciones de administración de energía en un servidor administrado.

Tabla 10-4. 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 has been stopped successfully` `(El system1 se ha detenido satisfactoriamente)`
Encender el servidor a partir de un estado de apagado	`->start /system1` `system1 has been started successfully` `(El system1 se ha iniciado satisfactoriamente)`

Reiniciar el servidor	->reset /system1 system1 has been reset successfully (El system1 ha sido restablecido satisfactoriamente)

Administración del SEL

La tabla 10-5 muestra ejemplos de cómo usar el SM-CLP para realizar operaciones relacionadas con el registro de sucesos del sistema en el sistema administrado.

Tabla 10-5. Operaciones de administración del SEL

Operación	Sintaxis
Ver el SEL	->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 SEL	->show/system1/sp1/logs1/record4 ufip =/system1/sp1/logs1/log1/record4 ->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 SEL	->delete /system1/sp1/logs1 All records deleted successfully

Navegación del punto de acceso de administrabilidad de destino

La tabla 10-6 muestra ejemplos de cómo usar el verbo **cd** para navegar el punto de acceso de administrabilidad. En todos los ejemplos, se asume que el destino predeterminado inicial es /.

Tabla 10-6. Operaciones de navegación del mapa de destino

Operación	Sintaxis
Desplazarse al sistema de destino y reiniciarlo	->cd system1 ->reset **NOTA:** El destino predeterminado actual es /.
Desplazarse al registro de destino y mostrar las anotaciones del registro	->cd system1 ->cd ps1 ->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 10-7 muestra ejemplos de cómo establecer las propiedades del iDRAC por medio de SM-CLP.

Tabla 10-7. Configuración de las propiedades de red del iDRAC con SM-CLP

Operación	Sintaxis
Desplazarse a la ubicación de las propiedades de la tarjeta de interfaz de red 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 será finalizada. Es posible que deba esperar varios minutos a que la actualización del firmware concluya.

4. Para verificar que se escribió 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 serie en paquetes de red. La implementación de la comunicación en serie en la LAN de iDRAC elimina la necesidad de tener una utilidad adicional pues la traducción de la comunicación 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 que 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 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 de 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 icono de desconexión de HyperTerminal.

Uso de la comunicación en serie en la LAN por medio de 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 comando siguiente 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 comunicación en serie en la LAN, 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 la comunicación en serie en la LAN 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 comunicación en serie en la LAN:

```
start /system1/sol1
```

Con esto se conectará al puerto 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, escriba <Ctrl>+. (mantenga presionada la tecla Ctrl, presione y suelte la tecla de punto y después suelte la tecla Ctrl). La sesión de SSH se cerrará.

Una vez que haya iniciado la comunicación en serie en la LAN, 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 con firmware versión 1.00

- Antes de comenzar
- Creación de un archivo de imagen iniciable
- Preparación para la instalación
- Instalación del sistema operativo
- 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 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 la red de su empresa.

Antes de comenzar

Antes de usar la utilidad iVM-CLI, asegúrese 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 archivos controladores requeridos
- Los archivos de imagen de inicio del sistema operativo

El archivo de imagen debe ser un CD de sistema operativo o una imagen ISO de CD/DVD, con un formato iniciable estándar en la industria.

Creación de un archivo de imagen iniciable

Antes de instalar el archivo de imagen en los sistemas remotos, asegúrese que un sistema admitido pueda iniciarse 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 a continuación proporcionan información específica para crear archivos de imagen para sistemas Windows y Linux.

Creación de un archivo de imagen para 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 de símbolo del sistema y escriba lo siguiente:

```
dd if=<dispositivo_de_entrada> of=<archivo_de_salida>
```

Por ejemplo:

```
dd if=/dev/sdc0 of=mycd.img
```

Creación de un archivo de imagen para sistemas Windows

Al momento de elegir una utilidad de replicador de datos para crear archivos de imagen de Windows, seleccione una utilidad que copie el archivo de imagen y los sectores de inicio de CD/DVD.

Preparación para la instalación

Configuración de los sistemas remotos

1. Cree una área compartida de red a la que la estación de administración pueda tener acceso.
2. Copie los archivos de sistema operativo en la área compartida 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, prepárelo. Incluya los programas o secuencias de comandos que se vayan a utilizar para los procedimientos de instalación del sistema operativo.

   Por ejemplo, para distribuir un sistema operativo Microsoft® Windows®, el archivo de imagen puede incluir programas que sean parecidos a los métodos de distribución que utiliza Microsoft Systems Management Server (SMS).

   Al momento de crear el archivo de imagen, haga lo siguiente:

   - Siga procedimientos estándares de instalación basada en red
   - Marque la imagen de instalación como "de sólo lectura" para asegurarse que cada sistema de destino se inicie y ejecute el mismo procedimiento de instalación

4. 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 conocer detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta de 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 ofrece las funciones de medios virtuales de la estación de administración al iDRAC.

La utilidad iVM-CLI ofrece las siguientes características:

NOTA: Cuando se virtualizan archivos de imagen de sólo lectura, es posible que las sesiones múltiples no compartan la misma imagen. Cuando se virtualizan unidades físicas, sólo una sesión puede acceder a una unidad física determinada a la vez.

- Los dispositivos de medios extraíbles o los archivos de imagen que sean consecuentes con los complementos de medios virtuales
- Terminación automática cuando la opción "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 los grupos de usuarios, de manera que también controla qué usuarios que 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 constituye un medio centralizado para ofrecer acceso sin privilegios administrativos y lleva un registro de todos los comandos de 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 los archivos léame, que proporcionan la información más reciente del producto 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 es finalizado manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, puede usar el Administrador de tareas para finalizar 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 una dirección IP o nombre de DDNS no válidos, aparecerá un mensaje de error y el comando finalizará.

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.

Dispositivo de disco o archivo de Imagen

`-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, incluso el número de partición del sistema de archivos montable, si se aplica (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 el archivo a suministrar los medios virtuales de disco.

Por ejemplo, un archivo de imagen se especifica como:

`-f c:\temp\mi_disqt.img` (sistema Windows)

`-f /tmp/mi_disqt.img` (sistema Linux)

Si el archivo no está protegido contra escritura, Medios virtuales puede escribir al archivo de imagen. Configure el sistema operativo para proteger contra escritura un archivo de imagen de disco que no debe ser sobrescrito.

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 proporciona una capacidad de protección contra escritura, utilice esta capacidad asegurarse que Medios virtuales no escribirá en los medios.

Omita este parámetro de la línea de comandos si no va a virtualizar discos flexibles. Si un valor no válido es descubierto, se muestra un mensaje de error y el comando se finaliza.

Dispositivo de CD/DVD o archivo de imagen

`-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 el archivo que ofrecerá los medios de CD/DVD-ROM virtuales:

Por ejemplo, un archivo de imagen se especifica como:

`-c c:\temp\mi_dvd.img` (sistemas Windows)

`-c /tmp/mi_dvd.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 descubre un valor no válido, un mensaje de error es puesto en la lista y el comando se finaliza.

Especifique al menos un tipo de medio (unidad de disquete o de CD/DVD) con el comando, a menos que sólo se proporcionen opciones de interruptor. De lo contrario, se muestra un mensaje de error y el comando se finaliza y genera un error.

Para mostrar la versión

-v

Este parámetro se usa para mostrar la versión de la utilidad iVM-CLI. Si no se proporciona ninguna otra opción que no sea de interruptor, el comando se finaliza sin generar un mensaje de error.

Para mostrar la ayuda

-h

Este parámetro muestra un resumen de los parámetros de la utilidad iVM-CLI. Si no se proporciona ninguna otra opción que no sea de interruptor, el comando se finaliza 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 no se incluye este parámetro 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: redirige los mensajes impresos de salida 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 iVM-CLI no lee en la entrada estándar (**stdin**). Por consiguiente, no se requiere la redirección de **stdin**.

- Ejecución en segundo plano: de manera predeterminada, la utilidad iVM-CLI se ejecuta en primer plano. Use las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en segundo plano. Por ejemplo, en un sistema operativo Linux, el signo "&" después del comando hace que el programa sea iniciado 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 = ningún error

1 = No se pudo conectar

2 = Error de línea de comandos de iVM-CLI

3 =

se perdió la conexión de firmware de RAC

Los mensajes de texto únicamente en inglés también se envían a los mensajes de error estándares siempre que se encuentren 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 con firmware versión 1.00

- Descripción
- Inicio de la utilidad de configuración del iDRAC
- Uso de la utilidad de configuración del iDRAC

Descripción

La utilidad de configuración del iDRAC es un entorno de configuración previo al inicio que permite ver y establezca 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 usted puede realizar con la utilidad de configuración del iDRAC también se pueden realizar por medio de otras utilidades que se incluyen con el iDRAC o el software OpenManage, incluso 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 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.
```

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 12-1. 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 la 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 host	Presione <Entrar> para modificarla. Introduzca el nombre del host para las alertas de captura de sucesos de plataforma.
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, con lo que 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 12-2. 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 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 sino 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?

< NO (Cancel) >

< YES (Continue) >
```

```
(Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Desea 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 anotación para ir directamente a la anotación. 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> no ignorar los cambios que hizo.

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 con firmware versión 1.00

- La seguridad es lo primero: para usted y su sistema
- Indicadores de problemas
- Herramientas para solución de problemas
- Solución de problemas y preguntas frecuentes

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 sólo las puede realizar un técnico de servicio certificado. 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. Los daños ocasionados por reparaciones que no hayan sido autorizadas por Dell no están cubiertos por la garantía. Lea y siga las instrucciones de seguridad que se incluyeron 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
- Suministros de energía

El indicador LED de la pantalla LCD del chasis resume el estado de todos los componentes del sistema. Si el LED permanece encendido en 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 de Dell CMC con firmware versión 1.0* para obtener ayuda relacionada con el uso de la pantalla LCD.

La tabla 13-1 describe el significado del comportamiento del indicador LED del servidor PowerEdge:

Tabla 13-1. Indicadores LED del servidor

Indicador LED	Significado
verde continuo	El servidor está encendido. La ausencia 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 13-2. Indicadores de problemas

Busque:	Acción:
Mensajes de alerta del software de administración de sistemas	Consulte la documentación del software de administración de sistemas.
Mensajes en el registro de sucesos del sistema	Consulte Consulta del registro de sucesos del sistema (SEL).
Mensajes en los códigos de la POST de arranque	Consulte Revisión de los códigos de la POST.
Mensajes en la pantalla de último bloqueo	Consulte Visualización de la pantalla de último bloqueo del sistema.
Mensajes en el registro del iDRAC	Consulte Cómo ver el 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.

- Revisión de la condición del sistema
- Revisión del registro de sucesos del sistema en busca de mensajes de error
- Revisión de los códigos de la POST
- Cómo ver la pantalla de último bloqueo
- Cómo ver el 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

Revisión 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 13-3 describe el significado de los indicadores de condición del sistema.

Tabla 13-3. 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 de signo de interrogación indica que el estado es desconocido.

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 13-3), la fecha y hora, y una descripción del suceso.
3. Para continuar, haga clic en el botón adecuado de la página **Registro de sucesos del sistema** (consulte la tabla 13-4).

Tabla 13-4. Botones de la página de SEL

Botón	Acción
Imprimir	Imprime el **registro de sucesos del sistema en el orden que aparece en la ventana.**
Borrar registro	Borra el **SEL**. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **SEL** en un directorio de su elección. **NOTA:** Si está utilizando Internet Explorer y tiene problemas al guardar, asegúrese de descargar la actualización de seguridad acumulativa para Internet Explorer, que se encuentra en el sitio web de asistencia de Microsoft®, en support.microsoft.com.
Actualizar	Recarga la página **SEL**.

Revisión de los códigos de la POST

La página **Códigos de la POST** muestra el último código de la autoprueba de encendido del sistema antes de iniciar el sistema operativo. Los códigos de la POST son indicadores de progreso del sistema BIOS que indican varias etapas de la secuencia de inicio desde el restablecimiento de la alimentación y permiten diagnosticar fallas relativas al inicio del sistema.

NOTA: Vea el texto para conocer los números de mensaje de códigos de la POST en la pantalla LCD o en el *Manual del propietario del hardware.*

Para ver los códigos de la POST, realice los pasos siguientes:

1. Haga clic en **Sistema**, en la ficha **Registros** y después en **Códigos de la POST**.

   La página **Códigos de la POST** muestra un indicador de condición del sistema (consulte la tabla 13-3), un código hexadecimal y una descripción del código.
2. Para continuar, haga clic en el botón correspondiente de la página **Código de la POST** (consulte la tabla 13-5).

Tabla 13-5. Botones de código de la POST

Botón	Acción
Imprimir	Imprime la página **Códigos de la POST.**
Actualizar	Vuelve a cargar la página **Códigos de la 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 de 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 13-6:

NOTA: Los botones **Guardar** y **Eliminar** no aparecerán si no hay ninguna pantalla de bloqueo guardada.

Tabla 13-6. Botones de página de 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 ser capturada 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 que la **Pantalla de último bloqueo** funcione correctamente. Consulte Configuración del servidor administrado para capturar la pantalla de último bloqueo para obtener información adicional.

Cómo ver el 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 de la tabla 13-7.

Tabla 13-7. Información de la página 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 13-8).

Tabla 13-8. Botones del registro del iDRAC

Botón	Acción
Imprimir	Imprime la página **Registro del iDRAC**.
Borrar registro	Borra las anotaciones del **Registro de iDRAC**. **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 del iDRAC** en un directorio de su elección.

	NOTA: Si está utilizando Internet Explorer y tiene problemas al guardar, asegúrese de descargar la actualización de seguridad acumulativa para Internet Explorer, ubicada en el sitio web de asistencia de Microsoft, en **support.microsoft.com**.
Actualizar	Vuelve a cargar la página **Registro del iDRAC**.

Visualización de información del sistema

La página **Resumen del sistema** muestra información acerca de 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 13-9 y la tabla 13-10 describen las propiedades del gabinete del sistema principal.

Tabla 13-9. Campos de 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 de host	Proporciona el nombre del sistema host.
Nombre del sistema operativo	Muestra el sistema operativo que se ejecuta en el sistema.

Tabla 13-10. 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, expresado en segundos, del temporizador de cuenta regresiva.

Integrated Dell Remote Access Controller

La tabla 13-11 describe las propiedades de iDRAC.

Tabla 13-11. Campos de información 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.
Actualización del firmware	Enumera la fecha en la que el firmware se actualizó 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 M1000-e 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 mientras usted no 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 permanezca encendido 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 -1213) que es parecido a las herramientas que incluyen 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 13-12 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 13-12. 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 la interfaz de red.
netstat	Muestra el contenido de la tabla de encaminamiento.
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 introducir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control en Internet) se envía a la dirección IP de destino basada en el contenido de tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo de iDRAC. Consulte gettracelog para obtener más información.

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 con la configuración de los permisos de usuarios.

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 13-13 ofrece información sobre las acciones de control de la alimentación.

3. Haga clic en **Aplicar** para realizar la acción seleccionada.

4. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 13-14.

Tabla 13-13. Acciones de control de alimentación

Encender el sistema	Enciende la alimentación del sistema (equivalente a oprimir el botón de encendido cuando el sistema 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 13-14. 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 13-15 contiene preguntas frecuentes sobre la solución de problemas.

Tabla 13-15. 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 Consulta del registro de sucesos del sistema (SEL) En SM-CLP: • Consulte Administración del SEL En la utilidad de configuración del iDRAC: • Consulte el 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 ayudarles 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 a través de una conexión serie local. Los comandos RACADM de CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía del*

	usuario del CMC con firmware versión 1.0 para ver 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, resalte **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: • Haga clic en **Sistema**→ **Acceso remoto**→ **CMC**. La dirección IP del CMC se muestra en la página **Resumen**. O BIEN • 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 CMC con firmware versión 1.0* para ver 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 Duplex = Negociación automática
La conexión de red del iDRAC no funciona.	• Asegúrese que el cable de la LAN esté conectado con el CMC. • Asegúrese que la LAN del iDRAC está activada.
Inserté el servidor en el chasis y presioné el botón de encendido, pero no pasó nada.	• 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. • 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, resalte **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 es así, siga las instrucciones que se describen en 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: • La memoria no está instalada o no se puede tener acceso a ella. • La CPU no está instalada o no se puede tener acceso a ella. • 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

Active Directory

Active Directory es un sistema centralizado y estandarizado que automatiza la administración de redes de datos de usuarios, seguridad y recursos distribuidos, y permite la operación con otros directorios. Active Directory está especialmente diseñado para entornos de sistema de red distribuidos.

AGP

Siglas de "Accelerated Graphics Port" (Puerto de gráficos acelerados), que es una especificación de bus que permite a las tarjetas de gráficos tener un acceso más rápido a la memoria del sistema principal.

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

BIOS

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 a varias unidades funcionales en un equipo. Los buses reciben su nombre por el tipo de datos que llevan, por ejemplo, bus de datos, bus de direcciones o bus PCI.

CA

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis fiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Una vez que la CA recibe la CSR, revisan y verifican la información que contiene la CSR. Si el candidato cumple los estándares de seguridad de la CA, 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 iDRAC o el CMC que contiene información sobre los cambios de estado en el servidor administrado o sobre problemas potenciales de hardware.

CD

Abreviatura de disco compacto.

CHAP

Siglas de "Challenge-Handshake Authentication Protocol" (Protocolo de autentificación de establecimiento de conexión), que es un método de autentificación usado por 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).

CMC

Abreviatura de "Enclosure Management Controller" (controlador de administración de gabinete), que es la interfaz de controlador entre el iDRAC y el CMC del sistema administrado.

CSR

Siglas de "Certificate Signing Request" (solicitud de firma de certificado).

DDNS

Siglas de "Dynamic Domain Name System" (Sistema de nombres de dominio dinámico).

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 iDRAC mantiene un disco RAM en su memoria.

DLL

Abreviatura de Dynamic Link Library (Biblioteca de vínculo dinámico), que es una biblioteca de pequeños programas, 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" (Grupo de trabajo de administración distribuida).

DNS

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

DSU

Abreviatura de disk storage unit (unidad de almacenamiento en disco).

esquema ampliado

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

Estación de administración

La estación de administración es un sistema que accede de forma remota al iDRAC.

FQDN

Siglas de Fully Qualified Domain Names (Nombres de dominio totalmente calificados). Microsoft® Active Directory® sólo admite FQDN de 64 bytes o menos.

FSMO

"Flexible Single Master Operation" (Operación maestra única flexible). La manera en la que Microsoft garantiza la atomicidad de la operación de extensión.

GMT

Siglas 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

Siglas de "GRand Unified Bootloader", un nuevo y popular cargador de Linux.

GUI

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

iAMT

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

ICMB

Abreviatura de "Intelligent Enclosure Management Bus" (bus de administración de 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).

iDRAC

Siglas de Dell Remote Access Controller 5.

iDRAC

Siglas de Integrated Dell Remote Access Controller, el sistema de supervisión y control integrado en el chip de los servidores Dell 10G PowerEdge.

IP

Siglas 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 plataformas inteligentes), que es un bus usado en tecnología de administración de sistemas.

IPMI

Siglas de "Intelligent Platform Management Interface" (Interfaz de administración de plataformas inteligentes), que es una parte de la tecnología de administración de sistemas.

Kbps

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

LAN

Siglas de "local area network" (red de área local).

LDAP

Siglas de "Lightweight Directory Access Protocol" (Protocolo de acceso ligero de directorio).

LED

Siglas de "light-emitting diode" (diodo emisor de luz).

LOM

Abreviatura para "Local area network On Motherboard" (red de área local en la placa base).

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

MIB

Siglas de "management information base" (base de información de administración).

MII

Siglas de "Medios Interfaz Independiente" (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). Placa de circuitos de adaptador instalada en un equipo para proporcionar una conexión física a una red.

OID

Abreviatura de "Object Identifiers" (identificadores de objeto).

OSCAR

Siglas de "On Screen Configuration and Reporting" (Configuración e informes en pantalla). OSCAR es el menú que Avocent iKVM muestra cuando usted presiona <Impr Pant>. Éste permite seleccionar la consola del CMC o la consola del iDRAC para un servidor instalado en el CMC.

PCI

Siglas 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

Siglas de "remote access controller" (controlador de acceso remoto).

RAM

Siglas de "random-access memory" (memoria de acceso aleatorio). La RAM es una memoria de propósito general que se puede leer y en la que se puede escribir en los sistemas y en el iDRAC.

redirección de consola

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

registro de hardware

Registra los sucesos generados por el iDRAC y el CMC.

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.

SAP

Siglas de "Service Access Point" (punto de acceso de servicio).

SEL

Siglas de "system event log" (registro de sucesos del sistema).

servidor administrado

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

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 del sistema).

SSH

Abreviatura para "Secure Shell".

SSL

Abreviatura de secure sockets layer (capa de conexión segura).

TAP

Siglas de "Telelocator Alphanumeric Protocol" (Protocolo alfanumérico de telelocalizador), que es un protocolo usado para enviar solicitudes a un servicio de radiomensajes.

TCP/IP

Abreviatura para "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

Siglas 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.

UPS

Siglas de "uninterruptible power supply" (sistema de alimentación ininterrumpida).

USB

Siglas de "Universal Serial Bus" (bus en serie universal).

UTC

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

VLAN

Siglas de "Virtual Local Area Network" (Red virtual de área local).

VNC

Siglas de "virtual network computing" (cómputo de red virtual).

VT-100

Abreviatura para "Video Terminal 100" (terminal de vídeo 100), que se usa por los programas de emulación de terminal más comunes.

WAN

Siglas de "wide area network" (red de área amplia).

Regresar a la página de contenido