Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Notas y avisos

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

AVISO: Un AVISO indica la posibilidad de daños en el hardware o la pérdida de datos, y le informa cómo evitar el problema.

Julio de 2008

Regresar a la página de contenido

Generalidades del subcomando RACADM

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

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

---

help

NOTA: Para usar este comando, debe tener permiso para **Iniciar sesión en el DRAC 5**.

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

Tabla A-1. Comando help

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

Sinopsis

```
racadm help
```

```
racadm help <subcomando>
```

Descripción

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

Salida

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

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

arp

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

En la Tabla A-2 se describe el comando **arp**.

Tabla A-2. Comando arp

Comando	Definición
arp	Muestra el contenido de la tabla de ARP. Las anotaciones del ARP no se pueden agregar ni eliminar.

Sinopsis

```
racadm arp
```

Interfaces admitidas

- RACADM remota
- RACADM telnet/SSH/serie

---

clearasrscreen

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

En la Tabla A-3 se describe el subcomando **clearasrscreen**.

Tabla A-3. clearasrscreen

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

Sinopsis

```
racadm clearasrscreen
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

config

NOTA: Para usar el comando **getconfig**, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-4 se describen los subcomandos **config** y **getconfig**.

Tabla A-4. config / getconfig

Subcomando	Definición
config	Configura el DRAC 5.
getconfig	Obtiene la información de configuración de DRAC 5.

Sinopsis

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

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

Descripción

El subcomando **config** permite que el usuario establezca de manera individual los parámetros de configuración del DRAC 5 o que los procese en lotes como parte de un archivo de configuración. Si la información es diferente, el objeto de DRAC 5 se escribirá con el nuevo valor.

Entrada

En la Tabla A-5 se describen las opciones del subcomando **config**.

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

Tabla A-5. Opciones y descripciones del subcomando config

Opción	Descripción
-f	La opción **-f <nombre_de_archivo>** hace que **config** lea el contenido del archivo que se especifica en **<nombre_de_archivo>** y que configure el

	DRAC 5. El archivo debe contener los datos en el formato que se especifica en "Reglas del análisis".
-p	La opción **-p**, u opción de contraseña, hace que **config** elimine las anotaciones de contraseña que contiene el archivo de configuración **-f <*nombre_de_archivo*>** después de terminar la configuración.
-g	La opción **-g <*nombre_de_grupo*>**, u opción de grupo, se debe usar con la opción **-o**. El <*nombre_de_grupo*> especifica el grupo que contiene al objeto que se va a definir.
-o	La opción **-o <*nombre_de_objeto*> <*valor*>**, u opción de objeto, se debe usar con la opción **-g**. Esta opción especifica el nombre de objeto que se escribe con la cadena <*valor*>.
-i	La opción **-i <*índice*>**, u opción de índice, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. El <*índice*> es un número entero decimal de 1 a 16. El índice se especifica aquí mediante el valor del índice; no mediante un valor asignado.
-c	La opción **-c**, u opción de verificación, se usa con el subcomando **config** y permite que el usuario analice el archivo **.cfg** en busca de errores de sintaxis. Si se encuentran errores, se mostrará el número de línea y una breve descripción de lo que está incorrecto. No se realizarán operaciones de escritura en el DRAC 5. Esta opción es sólo una revisión.

Salida

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

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

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

Ejemplos

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

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

- `racadm config -f myrac.cfg`

  Configura o reconfigura el DRAC 5. El archivo **myrac.cfg** se puede crear a partir del comando **getconfig**. El archivo **myrac.cfg** también se puede editar manualmente siempre y cuando se sigan las reglas de sintaxis.

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

---

getconfig

Descripción del subcomando getconfig

El subcomando **getconfig** permite que el usuario recupere los parámetros de configuración de DRAC 5 de manera individual o se pueden recuperar todos los grupos de configuración de RAC y guardarse en un archivo.

Entrada

En la Tabla A-6 se describen las opciones del subcomando **getconfig**.

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

Tabla A-6. Opciones del subcomando getconfig

Opción	Descripción
-f	La opción **-f <*nombre_de_archivo*>** hace que getconfig escriba toda la configuración del RAC en un archivo de configuración. Este archivo se

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

Salida

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

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

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

Ejemplos

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

  Guarda todos los objetos de configuración de los grupos del RAC en **myrac.cfg**.

- `racadm getconfig -h`

  Muestra una lista de todos los grupos de configuración que están disponibles en el DRAC 5.

- `racadm getconfig -u root`

  Muestra las propiedades de configuración del usuario root.

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

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

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>
```

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

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

```
racadm getconfig -h
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

coredump

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

En la Tabla A-7 se describe el subcomando **coredump**.

Tabla A-7. coredump

Subcomando	Definición
coredump	Muestra el último volcado de núcleo del DRAC 5.

Sinopsis

```
racadm coredump
```

Descripción

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

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

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

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

Interfaces admitidas

- RACADM remota
- RACADM telnet/SSH/serie

---

coredumpdelete

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

En la Tabla A-8 se describe el subcomando **coredumpdelete**.

Tabla A-8. coredumpdelete

Subcomando	Definición
coredumpdelete	Borra el volcado de núcleo que está guardado en el DRAC 5.

Sinopsis

```
racadm coredumpdelete
```

Descripción

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

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

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

fwupdate

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

NOTA: Antes de comenzar la actualización del firmware, consulte "Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet (sistema cliente)" para obtener más instrucciones.

En la Tabla A-9 se describe el subcomando **fwupdate**.

Tabla A-9. fwupdate

Subcomando	Definición
fwupdate	Actualiza el firmware del DRAC 5.

Sinopsis

```
racadm fwupdate -s
```

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

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

Descripción

El subcomando **fwupdate** permite que los usuarios actualicen el firmware del DRAC 5. El usuario puede:

- Revisar el estado del proceso de actualización del firmware
- Actualizar el firmware del DRAC 5 de un servidor TFTP si se proporciona una dirección IP y una ruta de acceso opcional
- Actualizar el firmware del DRAC 5 desde el sistema local de archivos por medio de RACADM local

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

Entrada

En la Tabla A-10 se describen las opciones del subcomando **fwupdate**.

NOTA: La opción **-p** sólo se admite en la RACADM remota y no se admite con las consolas serie, Telnet o SSH.

Tabla A-10. Opciones del subcomando fwupdate

Opción	Descripción
-u	La opción **update** ejecuta una suma de comprobación del archivo de actualización del firmware y comienza el verdadero proceso de actualización. Esta opción se puede usar junto con las opciones **-g** o **-p**. Al final de la actualización, el DRAC 5 realiza un restablecimiento por software.
-s	La opción **status** muestra el estado actual del avance del proceso de actualización. Esta opción siempre se usa sin otras opciones.
-g	La opción **get** hace que el firmware obtenga el archivo de actualización del servidor TFTP. El usuario también debe especificar las opciones **-a** y **-d**. A falta de la opción **-a**, se leen los valores predeterminados de las propiedades que se encuentran en el grupo **cfgRemoteHosts** y se utilizan las propiedades **cfgRhostsFwUpdateIpAddr** y **cfgRhostsFwUpdatePath**.
-a	La opción **dirección IP** especifica la dirección IP del servidor TFTP.
-d	La opción **-d**, u opción de **directorio**, especifica el directorio en el servidor TFTP o en el servidor host del DRAC 5 donde reside el archivo de actualización del firmware.
-p	La opción **-p**, u opción de **colocar**, se utiliza para actualizar el archivo de firmware del DRAC 5 a partir del sistema administrado. La opción **-u** se debe usar con la opción **-p**.

Salida

Muestra un mensaje que indica qué operación se está ejecutando.

Ejemplos

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

  En este ejemplo, la opción **-g** hace que el firmware descargue el archivo de actualización de firmware de una ubicación (que se especifica con la opción **-d**) en el servidor TFTP en una dirección IP específica (que se indica con la opción **-a**). Después de que el archivo de imagen se descarga del servidor TFTP, el proceso de actualización comienza. Al terminar, el DRAC 5 se restablece.

  Si la descarga supera los 15 minutos y se agota el tiempo de espera, transfiera la imagen de actualización de firmware a la unidad local del servidor. Después, por medio de la redirección de consola, conecte el sistema remoto e instale el firmware de manera local por medio de racadm local.

- `racadm fwupdate -s`

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

- `racadm fwupdate -p -u -d c:\ <imágenes>`

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

- `racadm -r 192.168.0.120 -u root -p racpassword fwupdate -g -u -a 192.168.0.120 -d <imágenes>`

En este ejemplo, se utiliza RACADM para actualizar el firmware de un DRAC específico de manera remota por medio del nombre de usuario y contraseña del DRAC que se proporciona. La imagen se obtiene de un servidor TFTP.

NOTA: La opción **-p** no se admite en la interfaz RACADM remota para el subcomando fwupdate.

---

getssninfo

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-11 se describe el subcomando **getssninfo**.

Tabla A-11. Subcomando getssninfo

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

Sinopsis

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

Descripción

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

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

Entrada

En la Tabla A-12 se describen las opciones del subcomando **getssninfo**.

Tabla A-12. Opciones del subcomando getssninfo

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

Ejemplos

```
racadm getssninfo
```

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

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

Usuario	Dirección IP	Type	Consolas
root	192.168.0.10	Telnet	KVM virtual

```
racadm getssninfo -A

"root" 143.166.174.19 "Telnet" "NINGUNO"

racadm getssninfo -A -u *

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

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

---

getsysinfo

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-14 se describe el subcomando **racadm getsysinfo**.

Tabla A-14. getsysinfo

Comando	Definición
getsysinfo	Muestra la información del DRAC 5, la información del sistema y la información del estado de la vigilancia.

Sinopsis

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

Descripción

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

Entrada

En la Tabla A-15 se describen las opciones del subcomando **getsysinfo**.

Tabla A-15. Opciones del subcomando getsysinfo

Opción	Descripción
-d	Muestra la información del DRAC 5.
-s	Muestra la información del sistema
-w	Muestra la información de vigilancia
-A	Elimina la impresión de encabezados/etiquetas.

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

Salida

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

Ejemplo del mensaje de salida

```
RAC Information:
RAC Date/Time           = Thu Dec 8 20:01:33 2005
Firmware Version        = 1.0
Firmware Build          = 05.12.08
Last Firmware Update    = Thu Dec 8 08:09:36 2005



Hardware Version        = A00
Current IP Address      = 192.168.0.120
Current IP Gateway      = 192.168.0.1
Current IP Netmask      = 255.255.255.0
DHCP Enabled            = 0
MAC Address             = 00:14:22:18:cd:f9
Current DNS Server 1    = 0.0.0.0
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP   = 0
Register DNS RAC Name   = 0
DNS RAC Name            = rac-48192
Current DNS Domain      =


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


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

Ejemplos

```
racadm getsysinfo -A -s

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

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

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

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

racadm getsysinfo -w -s


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



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

Restricciones

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

---

getractime

NOTA: Para usar este comando, debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-16 se describe el subcomando **getractime**.

Tabla A-16. getractime

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

Sinopsis

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

Descripción

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

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

Salida

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

Ejemplo del mensaje de salida

```
racadm getractime

Thu Dec 8 20:15:26 2005



racadm getractime -d

20051208201542.000000
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

ifconfig

NOTA: Para usar este comando, debe tener permiso de **Ejecutar comandos de diagnóstico** o **Configurar el DRAC 5**.

En la Tabla A-17 se describe el subcomando **ifconfig**.

Tabla A-17. ifconfig

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

Sinopsis

```
racadm ifconfig
```

---

netstat

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

En la Tabla A-18 se describe el subcomando **netstat**.

Tabla A-18. netstat

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

Sinopsis

```
racadm netstat
```

Interfaces admitidas

- RACADM remota
- RACADM telnet/SSH/serie

---

ping

NOTA: Para usar este comando, debe tener permiso de **Ejecutar comandos de diagnóstico** o **Configurar el DRAC 5**.

En la Tabla A-19 se describe el subcomando **ping**.

Tabla A-19. ping

Subcomando	Definición
ping	Verifica que se puede acceder a la dirección IP de destino desde el DRAC 5 con el contenido de la tabla de enrutamiento actual. Se requiere una dirección IP de destino. Un paquete de eco de ICMP se envía a la dirección IP de destino en función del contenido de tabla de enrutamiento actual.

Sinopsis

```
racadm ping <dirección_IP>
```

Interfaces admitidas

- RACADM remota
- RACADM telnet/SSH/serie

---

setniccfg

NOTA: Para usar el comando **setniccfg**, debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-20 se describe el subcomando **setniccfg**.

Tabla A-20. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

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

Sinopsis

```
racadm setniccfg -d
```

```
racadm setniccfg -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 controlador.

- La opción **-d** activa DHCP para el puerto de administración de Ethernet (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 de números separados con puntos.

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

- La opción **-o** desactiva completamente el puerto de administración de Ethernet. <*dirección_IP*>, <*máscara_de_red*> y <*puerta_de_enlace*> se deben escribir como cadenas de números separados con puntos.

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

Salida

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

getniccfg

NOTA: Para usar el comando **getniccfg**, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-21 se describen los subcomandos **setniccfg** y **getniccfg**.

Tabla A-21. setniccfg / getniccfg

Subcomando	Definición
getniccfg	Muestra la configuración IP actual del controlador.

Sinopsis

```
racadm getniccfg
```

Descripción

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

Ejemplo del mensaje de salida

Si la operación no es satisfactoria, el subcomando getniccfg muestra el mensaje de error correspondiente. En caso contrario, si es satisfactoria, el mensaje de salida aparece con el formato siguiente:

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

getsvctag

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-22 se describe el subcomando **getsvctag**.

Tabla A-22. getsvctag

Subcomando	Definición
getsvctag	Muestra la etiqueta de servicio.

Sinopsis

```
racadm getsvctag
```

Descripción

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

Ejemplo

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

```
Y76TP0G
```

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

racdump

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

En la Tabla A-23 se describe el subcomando **racdump**.

Tabla A-23. racdump

Subcomando	Definición
racdump	Muestra información general y del estado de DRAC 5.

Sinopsis

```
racadm racdump
```

Descripción

El subcomando **racdump** ofrece un solo comando para obtener el estado de volcado y la información general de la placa de DRAC 5.

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

- Información general del sistema/RAC

- Volcado de núcleo
- Información de la sesión
- Información del proceso
- Información de la compilación de firmware

Interfaces admitidas

- RACADM remota
- RACADM telnet/SSH/serie

---

racreset

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-24 se describe el subcomando **racreset**.

Tabla A-24. racreset

Subcomando	Definición
racreset	Restablece el DRAC 5.

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

Sinopsis

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

Descripción

El subcomando **racreset** realiza un restablecimiento del DRAC 5. El suceso de restablecimiento se escribe en el registro del DRAC 5.

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

AVISO: Usted debe reiniciar el sistema después de ejecutar un restablecimiento forzado del DRAC 5, según se describe en la Tabla A-25.

En la Tabla A-25 se describen las opciones del subcomando **racreset**.

Tabla A-25. Opciones del subcomando racreset

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

Ejemplos

- `racadm racreset`

Inicia la secuencia de restablecimiento ordenado del DRAC 5.

- `racadm racreset hard`

Inicia la secuencia de restablecimiento forzado del DRAC 5.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

racresetcfg

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-26 se describe el subcomando **racresetcfg**.

Tabla A-26. racresetcfg

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

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

Descripción

El comando **racresetcfg** quita todas las anotaciones de propiedad de la base de datos que hayan sido configuradas por el usuario. La base de datos tiene propiedades predeterminadas para todas las anotaciones que se usan para restablecer la tarjeta a sus valores predeterminados originales. El DRAC 5 se restablece automáticamente después de restablecer las propiedades de la base de datos.

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

NOTA: Este subcomando también restablecerá el puerto COM y la velocidad en baudios predeterminada de la interfaz serie. Es posible que sea necesario reconfigurar los valores de la interfaz serie por medio de la pantalla de configuración del BIOS del servidor, a fin de acceder al RAC por medio del puerto serie.

---

serveraction

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

En la Tabla A-27 se describe el subcomando **serveraction**.

Tabla A-27. serveraction

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

Sinopsis

```
racadm serveraction <acción>
```

Descripción

El subcomando serveraction permite que los usuarios realicen operaciones de administración de la alimentación en el sistema host. En la Tabla A-28 se describen las opciones de control de alimentación de **serveraction**.

Tabla A-28. Opciones del subcomando serveraction

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

Salida

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

getraclog

NOTA: Para usar este comando, debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-29 se describe el comando **racadm getraclog**.

Tabla A-29. getraclog

Comando	Definición

getraclog -i	Muestra el número de anotaciones en el registro del DRAC 5.
getraclog	Muestra las anotaciones del registro del DRAC 5.

Sinopsis

```
racadm getraclog -i
```

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

Descripción

El comando **getraclog -i** muestra el número de anotaciones en el registro del DRAC 5.

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

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

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

Salida

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

Ejemplo del mensaje de salida

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

clrraclog

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

Sinopsis

```
racadm clrraclog
```

Descripción

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

---

getsel

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-30 se describe el comando **getsel**.

Tabla A-30. getsel

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

Sinopsis

```
racadm getsel -i
```

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

Descripción

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

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

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

-c: permite introducir el número máximo de anotaciones a mostrar.

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

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

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

-R: sólo se imprimen los datos sin procesar.

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

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

Salida

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

Por ejemplo,

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

clrsel

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

Sinopsis

```
racadm clrsel
```

Descripción

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

gettracelog

NOTA: Para usar este comando, se debe tener permiso para **Iniciar sesión en el DRAC 5**.

En la Tabla A-31 se describe el subcomando **gettracelog**.

Tabla A-31. gettracelog

Comando	Definición
gettracelog -i	Muestra el número de anotaciones en el registro de seguimiento del DRAC 5.
gettracelog	Muestra las anotaciones del registro de seguimiento del DRAC 5.

Sinopsis

```
racadm gettracelog -i
```

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

Descripción

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

-i: muestra el número de anotaciones que hay en el registro de seguimiento del DRAC 5

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

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

-c: especifica el número de anotaciones a mostrar

-s: especifica la anotación inicial a mostrar

-A: no muestra encabezados ni etiquetas

Salida

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

Por ejemplo,

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

sslcsrgen

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-32 se describe el subcomando **sslcsrgen**.

Tabla A-32. sslcsrgen

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

Sinopsis

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

```
racadm sslcsrgen -s
```

Descripción

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

Opciones

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

En la Tabla A-33 se describen las opciones del subcomando **sslcsrgen**.

Tabla A-33. Opciones del subcomando sslcsrgen

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

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

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

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

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

Restricciones

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

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

Ejemplos

```
racadm sslcsrgen -s
```

O bien:

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

sslcertupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-34 se describe el subcomando **sslcertupload**.

Tabla A-34. sslcertupload

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

Sinopsis

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

Opciones

En la Tabla A-35 se describen las opciones del subcomando **sslcertupload**.

Tabla A-35. Opciones del subcomando sslcertupload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertdownload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-36 se describe el subcomando **sslcertdownload**.

Tabla A-36. sslcertdownload

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

Sinopsis

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

Opciones

En la Tabla A-37 se describen las opciones del subcomando **sslcertdownload**.

Tabla A-37. Opciones del subcomando sslcertdownload

Opción	Descripción

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

sslcertview

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-38 se describe el subcomando **sslcertview**.

Tabla A-38. sslcertview

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

Sinopsis

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

Opciones

En la Tabla A-39 se describen las opciones del subcomando **sslcertview**.

Tabla A-39. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado que se va a descargar, ya sea un certificado de Microsoft Active Directory o un certificado de servidor.

	1 = certificado del servidor 2 = certificado de Microsoft Active Directory
-A	Evita la impresión de encabezados/etiquetas.

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1


Serial Number             : 00


Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : DRAC5 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)          : DRAC5 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
DRAC5 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

sslkeyupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-40 se describe el subcomando **sslkeyupload**.

Tabla A-40. sslkeyupload

Subcomando	Descripción
sslkeyupload	Carga una clave SSL del cliente al DRAC 5.

Sinopsis

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

Opciones

En la Tabla A-41 se describen las opciones del subcomando **sslkeyupload**.

Tabla A-41. Opciones del subcomando sslkeyupload

Opción	Descripción
-t	Especifica la clave que se va a cargar. 1 = certificado del servidor
-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 **sslkeyupload** muestra `0` cuando se ejecuta de manera satisfactoria y un valor distinto a cero cuando no se ejecuta satisfactoriamente.

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

krbkeytabupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-42 se describe el subcomando **krbkeytabupload**.

Tabla A-42. Subcomando kerbkeytabupload

Subcomando	Descripción
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.

Sinopsis

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

Opciones

En la Tabla A-43 se describen las opciones del subcomando **krbkeytabupload**.

Tabla A-43. Opciones del subcomando krbkeytabupload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

testemail

En la Tabla A-44 se describe el subcomando **testemail**.

Tabla A-44. Configuración de testemail

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

Sinopsis

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

Descripción

Envía un correo electrónico de prueba, del RAC a un destinatario determinado.

Antes de ejecutar el comando de correo electrónico de prueba, compruebe que el índice que se especifica en el grupo **cfgEmailAlert** de RACADM está habilitado y configurado correctamente. La Tabla A-45 muestra una lista y los comandos asociados con el grupo **cfgEmailAlert**.

Tabla A-45. Configuración de testemail

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

Opciones

En la Tabla A-46 se describen las opciones del subcomando **testemail**.

Tabla A-46. Subcomandos de testemail

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

Salida

Ninguno.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

testtrap

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

En la Tabla A-47 se describe el subcomando **testtrap**.

Tabla A-47. testtrap

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

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

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

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

La Tabla A-48 muestra una lista y los comandos asociados con el grupo **cfgIpmiPet**.

Tabla A-48. Comandos de cfgEmailAlert

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

Entrada

En la Tabla A-49 se describen las opciones del subcomando **testtrap**.

Tabla A-49. Opciones del subcomando testtrap

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

vmdisconnect

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

En la Tabla A-50 se describe el subcomando vmdisconnect.

Tabla A-50. vmdisconnect

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

Sinopsis

```
racadm vmdisconnect
```

Descripción

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

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

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

vmkey

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

En la Tabla A-51 se describe el subcomando vmkey.

Tabla A-51. vmkey

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

Sinopsis

```
racadm vmkey <acción>
```

Si *<acción>* se configura como reset, se restablecerá el tamaño predeterminado de 16 MB de la memoria flash virtual.

Descripción

Al cargar una imagen personalizada de memoria de medios virtuales al RAC, el tamaño de la memoria será el tamaño de la imagen. El subcomando vmkey se puede usar para restablecer el tamaño original predeterminado de la memoria, que es de 16 MB en el DRAC 5.

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

usercertupload

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-52 se describen las opciones del subcomando **usercertupload**.

Tabla A-52. usercertupload

Subcomando	Descripción
usercertupload	Carga un certificado de usuario o un certificado de CA de usuario del cliente al DRAC.

Sinopsis

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

Opciones

En la Tabla A-53 se describen las opciones del subcomando **usercertupload**.

Tabla A-53. Opciones del subcomando usercertupload

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

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

Restricciones

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

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remota

---

usercertview

NOTA: Para usar este comando, se debe tener permiso para **Configurar el DRAC 5**.

En la Tabla A-54 se describe el subcomando **usercertview**.

Tabla A-54. usercertview

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

Sinopsis

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

Opciones

En la Tabla A-55 se describen las opciones del subcomando **sslcertview**.

Tabla A-55. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado a mostrar; el certificado de usuario o el certificado de CA de usuario. 1 = certificado de usuario 2 = certificado de CA de usuario
-A	Evita la impresión de encabezados/etiquetas.
-i	Número de índice del usuario. Los valores válidos son de 1 a 6

Interfaces admitidas

- RACADM local
- RACADM remota
- RACADM telnet/SSH/serie

---

localConRedirDisable

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

En la Tabla A-56 se describe el subcomando localConRedirDisable.

Tabla A-56. localConRedirDisable

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

Sinopsis

```
racadm localConRedirDisable <opción>
```

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

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 del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

La base de datos de propiedades del DRAC 5 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 DRAC 5. Las secciones siguientes describen cada objeto e indican si el objeto se puede leer, escribir, o ambos.

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

```
abcdefghijklmnopqrstuvwxwz
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

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

---

idRacInfo

Este grupo contiene parámetros de pantalla para proporcionar información acerca de las características específicas del DRAC 5 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

Dell Remote Access Controller (DRAC) 5

Descripción

Usa una cadena de texto para identificar 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 servidores Dell PowerEdge."

Descripción

Una descripción de texto del tipo de RAC.

idRacVersionInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

"1.0"

Descripción

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

idRacBuildInfo (sólo lectura)

Valores legales

Cadena de hasta 16 caracteres ASCII.

Predeterminado

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

Descripción

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

idRacName (sólo lectura)

Valores legales

Cadena de hasta 15 caracteres ASCII.

Predeterminado

DRAC 5

Descripción

Un usuario asigna un nombre para identificar a este controlador.

idRacType (sólo lectura)

Predeterminado

6

Descripción

Identifica el tipo de controlador de acceso remoto como el DRAC 5.

---

cfgLanNetworking

Este grupo contiene parámetros para configurar la tarjeta de interfaz de red del DRAC 5.

Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca la tarjeta de interfaz de red del DRAC 5, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP de la tarjeta de interfaz de red del DRAC 5 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)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Especifica que el nombre de dominio DNS del RAC se debe asignar a partir del servidor DHCP de la red.

cfgDNSDomainName (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

Cadena de hasta 254 caracteres ASCII Al menos uno de los caracteres debe ser alfabético. Sólo se admiten caracteres alfanuméricos, '-' y '.'

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

Predeterminado

""

Descripción

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

cfgDNSRacName (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

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

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

Predeterminado

rac-etiqueta_de_servicio

Descripción

Muestra el nombre del RAC, que es rac-etiqueta_de_servicio (valor predeterminado). Este parámetro sólo es válido si **cfgDNSRegisterRac** se establece como 1 (TRUE).

cfgDNSRegisterRac (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

1 = Registra el nombre del DRAC 5 en el servidor DNS.

cfgDNSServersFromDHCP (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgDNSServer1 (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

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

Descripción

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

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

cfgDNSServer2 (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

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

cfgNicEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la controladora de interfaz de red (NIC) integrada. Si la tarjeta de interfaz de red está desactivada, ya no se podrá acceder a las interfaces de red remota hacia el RAC y éste sólo estará disponible a través de las interfaces local o remota de RACADM.

cfgNicIpAddress (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**. Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSE).

Valores legales

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

Predeterminado

192.168.0.120

Descripción

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

cfgNicNetmask (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**. Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSE).

Valores legales

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

Predeterminado

255.255.255.0

Descripción

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

cfgNicGateway (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**. Este parámetro sólo se puede configurar si el parámetro **cfgNicUseDhcp** se establece como 0 (FALSE).

Valores legales

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

Predeterminado

192.168.0.1

Descripción

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

cfgNicUseDhcp (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

NOTA: Si va a actualizar el sistema de manera remota, utilice el comando **setniccfg**.

cfgNicSelection (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (compartido)

1 (dedicado con protección contra fallas)

2 (dedicado)

Predeterminado

2

Descripción

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

Tabla B-1. Modos admitidos de cfgNicSelection

Modo	Descripción
Compartido	Se utiliza cuando la tarjeta integrada de interfaz de red del servidor host se comparte con el RAC en el servidor host. Este modo habilita las configuraciones para utilizar la misma dirección IP en el servidor host y el RAC para tener accesibilidad común en la red.
Compartido con protección contra fallas	Activa la capacidad para formar un equipo entre los controladores integrados de red del servidor host.
Dedicado	Especifica que la tarjeta de interfaz de red del RAC se utilice como tarjeta dedicada para accesibilidad remota.

cfgNicMacAddress (sólo lectura)

Valores legales

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

Predeterminado

La dirección MAC actual de la tarjeta de interfaz de red del RAC. Por ejemplo, "00:12:67:52:51:A3".

Descripción

La dirección MAC de la tarjeta de interfaz de red del RAC.

cfgNicVLanEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgNicVLanId (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 0 a 4094

Predeterminado

0

Descripción

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

cfgNicVLanPriority (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 0 a 7

Predeterminado

0

Descripción

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

---

cfgRemoteHosts

Este grupo contiene las propiedades que permiten la configuración de varios componentes remotos, lo que incluye el servidor SMTP de las alertas de correo electrónico y dirección IP del servidor TFTP para actualizaciones de firmware.

cfgRhostsSmtpServerIpAddr (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

0.0.0.0

Descripción

La dirección IP del servidor SMTP de red. El servidor SMTP transmite las alertas de correo electrónico desde el RAC si las alertas están configuradas y activadas.

cfgRhostsFwUpdateTftpEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

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

cfgRhostsFwUpdateIpAddr (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Una cadena que representa una dirección IP válida de servidor TFTP. Por ejemplo: `192.168.0.61`.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP del servidor TFTP de red que se utiliza para operaciones de actualización de firmware del RAC por TFTP.

cfgRhostsFwUpdatePath (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 255

Predeterminado

""

Descripción

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

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

---

cfgUserAdmin

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

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

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

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

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.

cfgUserAdminIpmiSerialPrivilege (lectura/escritura)

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

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 conexión serie de IPMI.

cfgUserAdminPrivilege (lectura/escritura)

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

Valores legales

0x0000000 a 0x00001ff, y 0x0

Predeterminado

0x0000000

Descripción

Esta propiedad especifica los privilegios de autoridad según funciones que se conceden al usuario. El valor se representa como máscara de bits que permite cualquier combinación de valores de privilegios. La Tabla B-2 describe las máscaras de bits de los privilegios de usuario.

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

Privilegio del usuario	Máscara de bits de privilegios
Iniciar sesión en el DRAC 5	0x0000001
Configurar el DRAC 5	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Ejemplos

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

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

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

cfgUserAdminUserName (lectura/escritura)

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

Valores legales

Cadena. Cantidad máxima de caracteres = 16

Predeterminado

""

Descripción

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

NOTA: Este valor de propiedad DEBE SER exclusivo respecto de otras instancias de usuario.

cfgUserAdminPassword (de sólo escritura)

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

Valores legales

Una cadena de hasta 20 caracteres ASCII.

Predeterminado

""

Descripción

La contraseña para este usuario. Las contraseñas de usuario están cifradas y no pueden ser vistas o mostradas después que se ha escrito esta propiedad.

cfgUserAdminEnable

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

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva un usuario individual.

cfgUserAdminSolEnable

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

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

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

Descripción

El índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgEmailAlertAddress (sólo lectura)

Valores legales

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

Predeterminado

""

Descripción

La dirección de correo electrónico del origen de la alerta.

cfgEmailAlertCustomMsg (sólo lectura)

Valores legales

Cadena. Cantidad máxima de caracteres = 32.

Predeterminado

""

Descripción

Especifica el mensaje personalizado que se enviará con la alerta.

---

cfgSessionManagement

Este grupo contiene parámetros para configurar el número de sesiones que se pueden conectar al DRAC 5.

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

cfgSsnMgtConsRedirMaxSessions (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 2

Predeterminado

2

Descripción

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

cfgSsnMgtRacadmTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 10 a 1920

Predeterminado

30

Descripción

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

cfgSsnMgtWebserverTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 60 a 1920

Predeterminado

300

Descripción

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

Si la sesión de servidor web expira, la sesión actual se cerrará.

cfgSsnMgtSshIdleTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

300

Descripción

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

Cuando la sesión de Secure Shell expire, aparecerá el siguiente mensaje de error sólo si 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 espera0
```

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

cfgSsnMgtTelnetTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (Sin tiempo de espera)

De 60 a 1920

Predeterminado

0

Descripción

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

Cuando la sesión de Telnet expire, aparecerá el siguiente mensaje de error sólo si 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 aparezca, el sistema regresará al nivel de comandos que generó la sesión de Telnet.

---

cfgSerial

Este grupo contiene parámetros de configuración para el puerto serie del DRAC 5.

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

cfgSerialBaudRate (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

9600, 28800, 57600, 115200

Predeterminado

57600

Descripción

Establece la velocidad en baudios en el puerto serie del DRAC 5.

cfgSerialConsoleEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgSerialConsoleQuitKey (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

CADENA

MaxLen = 2

Predeterminado

^\ (<Ctrl><\>)

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

Descripción

Esta tecla o combinación de teclas finaliza la redirección de consola de texto cuando se utiliza el comando **connect com2**. El valor **cfgSerialConsoleQuitKey** puede estar representado por:

- Valor ASCII: por ejemplo, "^a"

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

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

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

cfgSerialConsoleIdleTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 = Sin tiempo de espera

De 60 a 1920

Predeterminado

300

Descripción

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

cfgSerialConsoleNoAuth (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (activa la autenticación de inicio de sesión serie)

1 (desactiva la autenticación de inicio de sesión serie)

Predeterminado

0

Descripción

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

cfgSerialConsoleCommand (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Descripción

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

Predeterminado

""

Ejemplo

"connect com2"

cfgSerialHistorySize (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 0 a 8192

Predeterminado

8192

Descripción

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

cfgSerialSshEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de Secure Shell (SSH) en el DRAC 5.

cfgSerialTelnetEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgSerialCom2RedirEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Predeterminado

1

Valores legales

1 (TRUE)

0 (FALSE)

Descripción

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

---

cfgNetTuning

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

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

cfgNetTuningNicAutoneg (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (activado)

0 (desactivado)

Predeterminado

1

Descripción

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

cfgNetTuningNic100MB (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (10 Mb)

1 (100 Mb)

Predeterminado

1

Descripción

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

cfgNetTuningNicFullDuplex (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (Semidúplex)

1 (Dúplex completo)

Predeterminado

1

Descripción

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

cfgNetTuningNicMtu (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 576 a 1500

Predeterminado

1500

Descripción

El tamaño en bytes de la unidad de transmisión máxima que la tarjeta de interfaz de red del DRAC 5 utiliza.

cfgNetTuningTcpSrttDflt (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 6 a 384

Predeterminado

6

Descripción

El valor predeterminado base de tiempo de espera de recorrido sin obstrucciones para el tiempo de recorrido de la retransmisión de TCP expresado en unidades de medio segundo. (Escriba valores hexadecimales).

---

cfgOobSnmp

El grupo contiene parámetros para configurar las capacidades de captura y de agente SNMP del DRAC 5.

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

cfgOobSnmpAgentCommunity (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 31.

Predeterminado

público

Descripción

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

cfgOobSnmpAgentEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el agente SNMP en el RAC.

---

cfgRacTuning

Este grupo se utiliza para configurar distintas propiedades de configuración del RAC, por ejemplo, los puertos válidos y las restricciones de seguridad de los puertos.

cfgRacTuneHttpPort (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 10 a 65535

Predeterminado

80

Descripción

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

cfgRacTuneHttpsPort (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 10 a 65535

Predeterminado

443

Descripción

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

cfgRacTuneIpRangeEnable

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la función de validación de rango de direcciones IP del RAC.

cfgRacTuneIpRangeAddr

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena formateada como dirección IP. Por ejemplo: `192.168.0.44`.

Predeterminado

`192.168.1.1`

Descripción

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

cfgRacTuneIpRangeMask

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

`255.255.255.0`

Descripción

Cadena formateada como dirección IP. Por ejemplo: `255.255.255.0`.

cfgRacTuneIpBlkEnable

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgRacTuneIpBlkFailcount

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 2 a 16

Predeterminado

5

Descripción

La cantidad máxima de intentos fallidos de inicio de sesión dentro de la ventana antes de rechazar los intentos de inicio de sesión provenientes de la dirección IP.

cfgRacTuneIpBlkFailWindow

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 2 a 65535

Predeterminado

60

Descripción

Define el periodo en segundos dentro del que se cuentan los intentos fallidos. Cuando la antigüedad de los intentos fallidos supera este límite, el contador se restablece en cero

cfgRacTuneIpBlkPenaltyTime

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 2 a 65535

Predeterminado

300

Descripción

Define el periodo en segundos dentro del cual se rechazan las solicitudes de sesión provenientes de una dirección IP que tuvo exceso de intentos fallidos.

cfgRacTuneSshPort (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 65535

Predeterminado

22

Descripción

Especifica el número de puerto que se utiliza para la interfaz SSH del RAC.

cfgRacTuneTelnetPort (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 65535

Predeterminado

23

Descripción

Especifica el número de puerto que se utiliza para la interfaz Telnet del RAC.

cfgRacTuneRemoteRacadmEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la interfaz RACADM remota en el RAC.

cfgRacTuneConRedirEncryptEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Cifra el vídeo en una sesión de redirección de consola.

cfgRacTuneConRedirPort (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 65535

Predeterminado

5901

Descripción

Especifica el puerto que se debe utilizar para el tráfico de señales de teclado y mouse durante la actividad de redirección de consola con el RAC.

NOTA: Este objeto requiere de un restablecimiento del DRAC 5 antes de activarse.

cfgRacTuneConRedirVideoPort (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 65535

Predeterminado

5901

Descripción

Especifica el puerto que se debe utilizar para el tráfico de señales de vídeo durante la actividad de redirección de consola con el RAC.

NOTA: Este objeto requiere de un restablecimiento del DRAC 5 antes de activarse.

cfgRacTuneAsrEnable (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva la función de captura de la pantalla de bloqueo del RAC.

NOTA: Este objeto requiere de un restablecimiento del DRAC 5 antes de activarse.

cfgRacTuneDaylightOffset (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 0 a 60

Predeterminado

0

Descripción

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

cfgRacTuneTimezoneOffset (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De -720 a 780

Predeterminado

0

Descripción

Especifica la compensación de huso horario (en minutos) en relación al GMT/UTC que se utiliza para la hora del RAC. A continuación, se muestran algunas compensaciones comunes de huso horario en los Estados Unidos:

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

-420 (MST: hora estándar de las montañas)

-360 (CST: hora estándar del centro)

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

cfgRacTuneWebserverEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

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

cfgRacTuneLocalServerVideo (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (activa)

0 (desactiva)

Predeterminado

1

Descripción

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

cfgRacTuneLocalConfigDisable

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la capacidad que tiene un usuario local para configurar el DRAC 5 por medio de racadm local o mediante las utilidades de Dell OpenManage Server Administrator.

cfgRacTuneCtrlEConfigDisable

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la capacidad de desactivar la facultad del usuario local para configurar el DRAC 5 a partir de la ROM de opción de la POST de BIOS.

---

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 (Read/Write)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

""

Descripción

El nombre de host del sistema administrado.

ifcRacMnOsOsName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

""

Descripción

El nombre del sistema operativo del sistema administrado.

---

cfgRacSecurity

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

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

cfgRacSecCsrCommonName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica el nombre común (CN) de la CSR.

cfgRacSecCsrOrganizationName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

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

cfgRacSecCsrOrganizationUnit (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la unidad organizacional (OU) de la CSR.

cfgRacSecCsrLocalityName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la localidad (L) de la CSR.

cfgRacSecCsrStateName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

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

cfgRacSecCsrCountryCode (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 2.

Predeterminado

""

Descripción

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

cfgRacSecCsrEmailAddr (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Cadena. Cantidad máxima de caracteres = 254.

Predeterminado

""

Descripción

Especifica la dirección de correo electrónico de la CSR.

cfgRacSecCsrKeySize (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1024

2048

4096

Predeterminado

1024

Descripción

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

---

cfgRacVirtual

Este grupo contiene parámetros para configurar la función de medios virtuales del DRAC 5. Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgVirMediaAttached (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para Configurar el DRAC 5.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Este objeto se utiliza para conectar los dispositivos virtuales por medio del bus USB. Al conectar los dispositivos, el servidor reconocerá los dispositivos USB válidos de almacenamiento masivo. Esto es equivalente a conectar una unidad de disco o de CD-ROM USB local a un puerto USB del sistema. Cuando los dispositivos se conectan, usted puede conectarse a los dispositivos virtuales de manera remota por medio de la interfaz Web o la CLI del DRAC 5. Si asigna el valor de **0** a este objeto, hará que los dispositivos se desconecten del bus USB.

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

cfgVirAtapiSrvPort (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso de **Acceso a los medios virtuales**.

Valores legales

De 1 a 65535

Predeterminado

3669

Descripción

Especifica el número de puerto que se utiliza para las conexiones cifradas de medios virtuales con el RAC.

cfgVirAtapiSrvPortSsl (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

3669

Descripción

Establece el puerto que se utiliza para las conexiones de medios virtuales SSL.

cfgVirMediaKeyEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgVirMediaBootOnce (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (activado)

0 (desactivado)

Predeterminado

0

Descripción

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

NOTA: Para activar la función Iniciar una vez, acceda a la configuración del BIOS y modifique manualmente el orden de inicio durante el reinicio del sistema.

cfgFloppyEmulation (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (verdadero)

0 (falso)

Predeterminado

0

Descripción

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

---

cfgActiveDirectory

Este grupo contiene parámetros para configurar la función Active Directory del DRAC 5.

cfgADRacDomain (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

""

Descripción

El dominio de Active Directory donde reside el DRAC.

cfgADRacName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

""

Descripción

Nombre del DRAC según está registrado en el bosque de Active Directory.

cfgADEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgADSpecifyServerEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 ó 0 (verdadero o falso).

Predeterminado

0

Descripción

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

cfgADDomainController (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Dirección IP válida o nombre de dominio completo (FQDN)

Predeterminado

No hay valores predeterminados

Descripción

El DRAC 5 utiliza el valor que usted especifique para buscar nombres de usuario en el servidor LDAP.

cfgADGlobalCatalog (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

FQDN o dirección IP válida

Predeterminado

No hay valores predeterminados

Descripción

El DRAC 5 utiliza el valor que usted especifique para buscar nombres de usuario en el servidor de catálogo global.

cfgAODomain (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

FQDN o dirección IP válida

Formato

<dominio>:<IP o FQDN>

Predeterminado

No hay valores predeterminados

Descripción

El DRAC 5 utilizará el valor que especifique para buscar nombres de usuario en el objeto de asociación.

cfgADSmartCardLogonEnable (lectura / escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el inicio de sesión Smart Card en el DRAC 5.

cfgADCRLEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la revisión de la lista de revocación de certificado (CRL) para los usuarios de Smart Card basados en Active Directory.

cfgADAuthTimeout (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 15 a 300

Predeterminado

120

Descripción

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

cfgADRootDomain (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

""

Descripción

Dominio raíz del bosque de dominios.

cfgADType (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 = Activa el esquema ampliado con Active Directory.

2 = Activa el esquema estándar con Active Directory.

Predeterminado

1 = Esquema ampliado

Descripción

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

cfgADSSOEnable (lectura/ escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

---

cfgStandardSchema

Este grupo contiene parámetros para configurar los valores del esquema estándar.

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

Número entero de 1 a 5.

Descripción

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

cfgSSADRoleGroupName (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

(vacío)

Descripción

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

cfgSSADRoleGroupDomain (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

(vacío)

Descripción

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

cfgSSADRoleGroupPrivilege (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

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

Predeterminado

(vacío)

Descripción

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

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

Privilegio de grupo de funciones	Máscara de bits
Iniciar sesión en el DRAC 5	0x00000001
Configurar el DRAC 5	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a redirección de consola	0x00000020
Acceder a los medios virtuales	0x00000040
Probar alertas	0x00000080
Ejecutar comandos de depuración	0x00000100

---

cfgIpmiSerial

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

cfgIpmiSerialConnectionMode (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (terminal)

1 (básico)

Predeterminado

1

Descripción

Cuando la propiedad **cfgSerialConsoleEnable** del DRAC 5 se establece como 0 (desactivada), el puerto serie del DRAC 5 se convierte en el puerto serie de IPMI. Esta propiedad determina el modo definido por IPMI del puerto serie.

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

cfgIpmiSerialBaudRate (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

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

cfgIpmiSerialChanPrivLimit (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSerialFlowControl (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (ninguno)

1 (CTS/RTS)

2 (XON/XOFF)

Predeterminado

1

Descripción

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

cfgIpmiSerialHandshakeControl (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

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

cfgIpmiSerialLineEdit (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

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

cfgIpmiSerialEchoControl (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

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

cfgIpmiSerialDeleteControl (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

0

Descripción

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

cfgIpmiSerialNewLineSequence (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (ninguno)

1 (CR-LF)

2 (NULO)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Predeterminado

1

Descripción

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

cfgIpmiSerialInputNewLineSequence (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (<ENTRAR>)

1 (NULO)

Predeterminado

1

Descripción

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

---

cfgIpmiSol

Este grupo se utiliza para configurar las capacidades de Conexión serie en la LAN del sistema.

cfgIpmiSolEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva la Conexión serie en la LAN (SOL).

cfgIpmiSolBaudRate (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

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

cfgIpmiSolMinPrivilege (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSolAccumulateInterval (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 255.

Predeterminado

10

Descripción

Especifica la cantidad de tiempo normal que el BMC espera antes de transmitir un paquete parcial de datos de caracteres SOL. Este valor consta de incrementos de 5 ms basados en unos.

cfgIpmiSolSendThreshold (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 255

Predeterminado

255

Descripción

El valor del límite de umbral de SOL.

---

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de la consola serie de IPMI en la LAN.

cfgIpmiLanPrivLimit (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

0

Descripción

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

cfgIpmiLanAlertEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

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

cfgIpmiEncryptionKey (lectura/escritura)

NOTA: Para ver o modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5** y privilegios de administrador.

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)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

Una cadena de hasta 18 caracteres.

Predeterminado

"public"

Descripción

El nombre de comunidad SNMP para las capturas.

---

cfgIpmiPef

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

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

cfgIpmiPefName (sólo lectura)

Valores legales

Cadena. Cantidad máxima de caracteres = 255.

Predeterminado

El nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de sucesos de plataforma.

cfgIpmiPefIndex (sólo lectura)

Valores legales

De 1 a 17

Predeterminado

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

Descripción

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

cfgIpmiPefAction (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (ninguno)

1 (apagar)

2 (restablecer)

3 (realizar ciclo de encendido)

Predeterminado

0

Descripción

Especifica la acción que se ejecuta en el sistema administrado cuando se presenta una alerta.

cfgIpmiPefEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva un filtro de sucesos de plataforma específico.

---

cfgIpmiPet

Este grupo se utiliza para configurar las capturas de sucesos de plataforma en el sistema administrado.

cfgIpmiPetIndex (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

De 1 a 4

Predeterminado

El valor de índice correspondiente.

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

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 sistema administrado.

cfgIpmiPetAlertEnable (lectura/escritura)

NOTA: Para modificar esta propiedad, debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva una captura específica.

Regresar a la página de contenido

Regresar a la página de contenido

Interfaces admitidas de RACADM

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

La tabla a continuación contiene una descripción general de los subcomandos de RACADM y la compatibilidad correspondiente de los mismos con interfaces.

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

Subcomando	Telnet/SSH/serie	RACADM local	RACADM remota
arp	✓	✗	✓
clearascreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
sslkeyupload	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓

vmkey	✔	✔	✔
usercertupload	✘	✔	✔
usercertview	✔	✔	✔
localConRedirDisable	✘	✔	✘
✔ = compatible; ✘ = no compatible			

Regresar a la página de contenido

Regresar a la página de contenido

Generalidades del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Dell™ Remote Access Controller 5 (DRAC 5) es una solución en hardware y software para administración de sistemas diseñada para proporcionar funciones de administración remota, recuperación ante fallas del sistema y de control de alimentación para los sistemas Dell.

La comunicación con el Controlador de administración de la placa base (BMC) del sistema permite configurar el DRAC 5 (si está instalado) para enviar alertas por correo electrónico sobre advertencias o errores relacionados con voltajes, temperaturas, intromisiones y velocidad del ventilador. El DRAC 5 también registra datos de sucesos, así como la pantalla de bloqueo más reciente (sólo para sistemas con el sistema operativo Microsoft® Windows®) para ayudarle a diagnosticar la causa probable del bloqueo del sistema.

El DRAC 5 incorpora su propio microprocesador y su propia memoria, y se alimenta del sistema en el que está instalado. Es posible que el módulo del DRAC 5 esté preinstalado en el sistema o está disponible de forma independiente en un paquete.

Para comenzar con el DRAC 5, consulte "Para comenzar con el DRAC 5".

Lo nuevo en esta publicación del DRAC 5

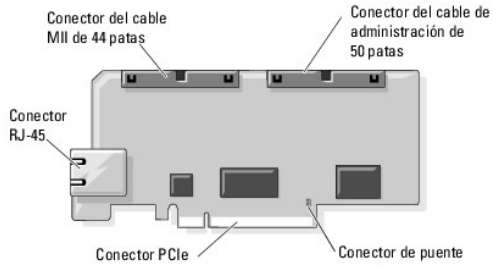
Para este lanzamiento, la versión 1.40 del firmware del DRAC 5:

- Ofrece compatibilidad para la autentificación en Microsoft Active Directory® mediante tarjeta inteligente
- Brinda compatibilidad para establecer conexión con el DRAC 5 mediante inicio de sesión único
- Ofrece sensores para supervisar el consumo de energía. El DRAC 5 utiliza estos datos para mostrar el consumo de energía del sistema a través de diagramas y estadísticas.
- Brinda una función de reproducción de video para ayudar a los administradores a visualizar los registros de POST e inicio del sistema operativo correspondientes a los sistemas administrados
- Ofrece compatibilidad mejorada para SM–CLP

Especificaciones y funciones del DRAC 5

La Figura 1-1 muestra el hardware del DRAC 5.

Figura 1-1. Componentes de hardware del DRAC 5



Especificaciones del DRAC 5

Especificaciones de alimentación

La Tabla 1-1 muestra una lista de los requisitos de alimentación del DRAC 5.

Tabla 1-1. Especificaciones de la alimentación del DRAC 5

Alimentación del sistema
1,2 A en auxiliar de +3,3 V (máxima)
550 mA en principal de +3,3 V (máxima)
0 mA en principal de +5 V (máxima)

Conectores

NOTA: Las instrucciones de instalación del hardware del DRAC 5 se encuentran en el documento *Instalación de una tarjeta de acceso remoto* o en la *Guía de instalación y solución de problemas* que se incluye con el sistema.

El DRAC 5 incluye un NIC integrado de 10/100 Mbps con conector RJ-45, un cable de administración de 50 patillas y un cable MII de 44 patillas. Consulte la Figura 1-1 para conocer los conectores de cables del DRAC 5.

El cable de administración de 50 patillas es la interfaz principal del DRAC que brinda conectividad a USB, conexión serie, vídeo y bus de circuito inter integrado (I2C). El cable MII de 44 patillas conecta el NIC del DRAC con la placa base del sistema. El conector RJ-45 conecta el NIC del DRAC a una conexión fuera de banda cuando el DRAC 5 está configurado en el modo **NIC dedicado**.

En función de sus requisitos, puede usar los cables de administración y MII para configurar el DRAC en tres modos separados. Consulte "Modos del DRAC" para obtener más información.

Puertos del DRAC 5

La Tabla 1-2 identifica los puertos que el DRAC 5 utiliza para detectar una conexión de servidor. La Tabla 1-3 identifica los puertos que el DRAC 5 utiliza como clientes. Esta información es necesaria cuando se abren puertos en los servidores de seguridad para tener acceso remoto al DRAC 5.

Tabla 1-2. Puertos de detección de servidor del DRAC 5

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

Tabla 1-3. Puertos de cliente del DRAC 5

Número de puerto	Función
25	SMTP

53	DNS
68	Dirección IP asignada por DHCP
69	TFTP
162	captura SNMP
636	LDAPS
3269	LDAPS para catálogo global (GC)

Conexiones de acceso remoto admitidas

La Tabla 1-4 muestra una lista de las funciones de conexión.

Tabla 1-4. Conexiones de acceso remoto admitidas

Conexión	Características
NIC del DRAC 5	• Ethernet 10/100 Mbps • Compatibilidad con DHCP • Notificación de sucesos de correo electrónico y capturas SNMP • Interfaz de red dedicada para la interfaz basada en web del DRAC 5 • Compatibilidad con la consola Telnet/SSH y los comandos de CLI de RACADM que incluyen los comandos de inicio de sistema, restablecimiento, encendido y apagado.
Puerto serie	• Compatibilidad con la consola serie y los comandos de CLI de RACADM que incluyen los comandos de inicio de sistema, restablecimiento, encendido y apagado. • Compatibilidad para la redirección de consola de sólo texto para un emulador de terminal o terminal VT-100

Funciones estándares del DRAC 5

El DRAC 5 proporciona las siguientes funciones:

- Autenticación de dos factores, gracias al inicio de sesión de tarjeta inteligente. La autenticación de dos factores se basa en lo que los usuarios tienen (tarjeta inteligente) y lo que conocen (PIN).
- Autenticación de usuarios por medio de Microsoft Active Directory (opcional) o identificaciones y contraseñas de usuarios guardadas en hardware
- Autoridad en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de identificación de usuario y contraseña por medio de la interfaz basada en web o de la CLI de RACADM
- Registro de Sistema de nombres de dominio dinámico (DNS)
- Administración y supervisión de sistemas remotos a través de una interfaz basada en web, conexión en serie, RACADM remota o conexión Telnet.
- Compatibilidad con la autenticación de Active Directory: centraliza todas las identificaciones y contraseñas de usuario del DRAC 5 en Active Directory por medio del esquema estándar y del esquema ampliado.
- Redirección de consola: proporciona funciones de teclado, vídeo y mouse al sistema remoto.
- Medios virtuales: activa un sistema administrado para acceder a la unidad de medios en la estación de administración.
- Acceso a los registros de sucesos del sistema: brinda acceso al registro de sucesos del sistema, el registro del DRAC 5 y la pantalla de último bloqueo del sistema que está bloqueado o que no responde. Este acceso es independiente del estado del sistema operativo.
- Integración del software de Dell OpenManage: permite ejecutar la interfaz basada en web del DRAC 5 de Dell OpenManage Server Administrator o IT Assistant.
- Alerta de RAC: envía alertas sobre problemas potenciales del nodo administrado por medio de mensajes de correo electrónico o una captura SNMP que utilice la configuración de NIC **Dedicada**, **Compartida con protección contra fallas** o **Compartida**.
- Configuración local y remota: brinda configuración local y remota por medio de la utilidad de línea de comandos de RACADM.
- Administración de la alimentación remota: proporciona funciones de administración de la alimentación remota proveniente de una consola de administración, por ejemplo, apagado y restablecimiento.
- Compatibilidad con IPMI.
- Administración basada en normas con IPMI a través de LAN y SM-CLP.
- Sensores para supervisar el consumo de energía. El DRAC 5 utiliza estos datos para representar el consumo de energía del sistema a través de diagramas y estadísticas.
- Cifrado de Capa de conexión segura (SSL): brinda administración segura de sistemas remotos por medio de la interfaz basada en web.
- Administración de seguridad a nivel de contraseña: evita el acceso no autorizado a un sistema remoto.
- Autoridad basada en funciones: brinda la capacidad de asignar permisos para distintas tareas de administración de sistemas.

Otros documentos útiles

Además de esta *Guía del usuario*, los documentos a continuación proporcionan información adicional sobre la configuración y operación del DRAC 5 en el sistema:

- La ayuda en línea del DRAC 5 proporciona información acerca de la utilización de la interfaz basada en web.
- La *Guía del usuario de Dell OpenManage™ IT Assistant* ofrece información sobre IT Assistant.
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- La *Guía de referencia de SNMP de Dell OpenManage Server Administrator* documenta la base de información de administración (MIB) de SNMP de Server Administrator. La MIB define las variables que amplían la MIB estándar para cubrir las capacidades de los agentes de systems management.
- La *Guía del usuario del controlador de administración de la placa base de Dell OpenManage* contiene información sobre cómo configurar el Controlador de administración de la placa base (BMC), cómo configurar el sistema administrado con la utilidad de administración del BMC e información adicional del BMC.
- La *Guía del usuario de Dell Update Packages* proporciona información acerca de cómo obtener y usar los Dell Update Packages como parte de su estrategia de actualización del sistema.
- La *Matriz de compatibilidad de software de los sistemas Dell* proporciona información sobre varios de los sistemas Dell, los sistemas operativos admitidos por estos sistemas y los componentes de Dell OpenManage que pueden estar instalados en estos sistemas.

Los documentos de sistema siguientes también están disponibles para proporcionar más información sobre el sistema en el que está instalado el DRAC 5:

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

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

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

Regresar a la página de contenido

Regresar a la página de contenido

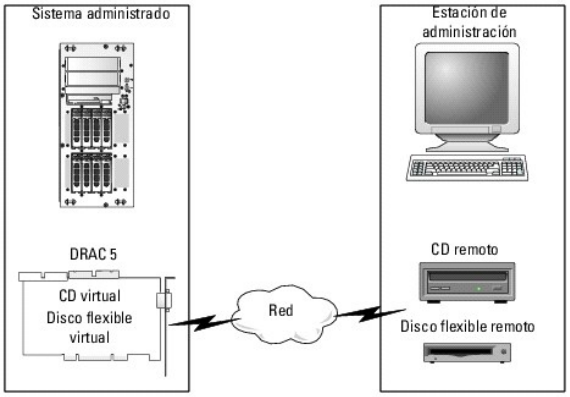
Uso y configuración de los medios virtuales

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Información general

La función de medios virtuales proporciona al sistema administrado una unidad de CD virtual que puede usar medios estándar de cualquier lugar de la red. La Figura 10-1 muestra la arquitectura general de los medios virtuales.

Figura 10-1. Arquitectura general de medios virtuales



Usando Medios virtuales, los administradores pueden iniciar los sistemas administrados, instalar aplicaciones, actualizar archivos controladores, o hasta instalar nuevos sistemas operativos remotamente desde las unidades de CD/DVD y disco virtuales.

NOTA: Los medios virtuales requieren una amplitud de banda de red mínima disponible de 128 Kbps.

El sistema administrado está configurado con una tarjeta DRAC 5. Las unidades de CD y de disco flexible virtuales son dos dispositivos electrónicos incorporados en el DRAC 5 que son controlados por el firmware del DRAC 5. Estos dos dispositivos están presentes en el sistema operativo del sistema administrado y en el BIOS en todo momento, sin importar si los medios virtuales están conectados o desconectados.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando se ejecuta el explorador de RAC la primera vez y usted accede a la página de medios virtuales, el complemento de medios virtuales se descarga del servidor web y se instala automáticamente en la estación de administración. El complemento de medios virtuales se debe instalar en la estación de administración para que el componente de medios virtuales funcione correctamente.

Cuando los medios virtuales están conectados, todas las solicitudes de acceso a las unidades virtuales de CD/disco flexible provenientes del sistema administrado se dirigen a la estación de administración a través de la red. La conexión de los medios virtuales es idéntica a la inserción de medios en los dispositivos virtuales. Cuando los medios virtuales no están conectados, los dispositivos virtuales en el sistema administrado aparecen como dos unidades sin medios instalados en ellas.

La Tabla 10-1 lista las conexiones compatibles de unidades ópticas virtuales y de disco flexible virtuales.

NOTA: Cambiar medios virtuales mientras están conectados podría detener la secuencia de inicio de sistema.

Tabla 10-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco flexible virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 pulgadas con disquete de 1,44 pulgadas	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disco flexible USB con un disquete de 1,44 pulgadas	Archivo de imagen de CD-ROM en formato ISO9660
Imagen de disco flexible de 1,44 pulgadas	Unidad de CD-ROM USB con disco CD-ROM.

Instalación del complemento de medios virtuales

El complemento explorador de medios virtuales se debe instalar en la estación de administración para usar la función de medios virtuales. Después de abrir la interfaz de usuario del DRAC 5 y de abrir la página de medios virtuales, el explorador descarga automáticamente el complemento, si es necesario. Si el complemento se instala correctamente, la página de medios virtuales muestra una lista de los disquetes y los discos ópticos que se conectan a la unidad virtual.

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 ActiveX. Establezca la seguridad del explorador en el nivel **Medio** o en un nivel inferior para permitir que Internet Explorer descargue e instale los controles ActiveX firmados.

Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

Además, debe tener derechos de administrador para instalar y utilizar el componente de medios virtuales. Antes de instalar el control ActiveX, es posible que Internet Explorer muestre una advertencia de seguridad. Para completar el procedimiento de instalación del control ActiveX, acepte el control ActiveX cuando Internet Explorer muestre la advertencia de seguridad.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión compatible de Mozilla o Firefox. Si el complemento de medios virtuales no está instalado o si hay una versión nueva, aparecerá un cuadro de diálogo durante el procedimiento de instalación para confirmar la instalación del complemento en la estación de administración. Compruebe que la identificación del usuario que ejecuta el explorador tenga permiso de escritura en el árbol de directorio del explorador. Si la identificación de usuario no tiene permiso de escritura, usted no podrá instalar el complemento de medios virtuales.

Consulte la *Matriz de compatibilidad del software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com** para obtener más información.

Ejecución de los medios virtuales

AVISO: No ejecute un comando racreset cuando esté ejecutando una sesión de medios virtuales. De lo contrario, se pueden presentar resultados inesperados, incluso la pérdida de datos.

A través de los medios virtuales, usted puede "virtualizar" una unidad o imagen de disquete, habilitar una imagen de disco flexible, una unidad de disco flexible o una unidad óptica en la consola de administración para que se convierta en una unidad disponible en el sistema remoto.

Configuraciones compatibles de medios virtuales

Puede activar los medios virtuales para una unidad de disco flexible y una unidad de discos ópticos. Sólo se puede virtualizar una unidad a la vez por cada tipo de medio.

Las unidades de disco flexible que se admiten incluyen una imagen de unidad de disco flexible o una unidad de disco flexible disponible. Las unidades ópticas que se admiten incluyen un máximo de una unidad óptica disponible o un archivo de imagen ISO.

Ejecución de los medios virtuales por medio de la interfaz web de usuario

Conexión de los medios virtuales

Abra un explorador de web compatible en la estación de administración. Consulte la *Matriz de compatibilidad del software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com** para obtener más información

AVISO: La redirección de consola y los medios virtuales sólo admiten exploradores de web de 32 bits. El uso de exploradores de web de 64 bits puede producir resultados inesperados o la falla de las operaciones.

2. Conéctese e inicie sesión en el DRAC 5. Consulte "Acceso a la interfaz basada en web" para obtener más información.
3. Haga clic en la ficha **Medios** y después haga clic en **Medios virtuales**.

La página **Medios virtuales** muestra las unidades de cliente que se pueden hacer virtuales.

NOTA: Es posible que aparezca **Archivo de imagen de disco flexible** bajo **Unidad de disco flexible** (si se aplica), pues este dispositivo se puede hacer un disco flexible virtual. Puede seleccionar una unidad óptica y un disco flexible al mismo tiempo o una sola unidad.

NOTA: Las letras de unidad de los dispositivos virtuales en el sistema administrado no coinciden con las letras de unidades físicas en la estación de administración.

4. Si el sistema lo solicita, siga las instrucciones que aparecen en la pantalla para instalar el complemento de medios virtuales.
5. En el cuadro **Atributo**, realice los siguientes pasos:
   a. En la columna **Valor**, compruebe que el valor de estado **Conectar/desconectar** sea **Conectado**.

      Si el valor es **Desconectado**, realice los pasos siguientes:

      - En la ficha **Medios**, haga clic en **Configuración**.
      - En la columna **Valor**, compruebe que la casilla **Conectar medios virtuales** esté seleccionada.
      - Haga clic en **Aplicar cambios**.
      - En la ficha **Medios virtuales**, haga clic en **Medios virtuales**.
      - En la columna **Valor**, compruebe que el valor de estado **Conectar/desconectar** sea **Conectado**.

   b. Compruebe que el valor de **Estado actual** sea **No conectado**. Si el campo Valor muestra "conectado", usted deberá desconectar la imagen o unidad antes de volver a conectarla. Este estado indica el estado actual de la conexión de los medios virtuales únicamente en la interfaz actual basada en web.

   c. Asegúrese que el valor de Sesión activa sea Disponible. Si el campo Valor muestra En uso, usted deberá esperar a que la sesión actual de medios virtuales se libere o deberá terminarla de la siguiente manera: seleccione la ficha Administración de sesión en Acceso remoto y termine la sesión activa de medios virtuales. Sólo se permite una sesión activa de medios virtuales a la vez. Esta sesión pudo haber sido creada por cualquier interfaz basada en web o utilidad VM-CLI.

   d. Seleccione la casilla **Cifrado activado** para establecer una conexión cifrada entre el sistema remoto y la estación de administración (si así lo desea).
6. Si va a virtualizar una imagen de disco flexible o una imagen ISO, seleccione **Archivo de imagen de disco flexible** o **Archivo de imagen ISO** e introduzca o desplácese hacia el archivo de imagen que desea hacer virtual.

Si va a virtualizar una unidad de disco flexible o una unidad óptica, seleccione el botón que se encuentra junto a las unidades que desea hacer virtuales.

7. Haga clic en **Conectar**.

Si la conexión se autentica, el estado de la misma cambiará a **Conectado** y aparecerá una lista de todas las unidades conectadas. Todas las imágenes de disquete y unidades que seleccione estarán disponibles en la consola del sistema administrado como si fueran unidades reales.

NOTA: Es posible que la letra asignada de unidad virtual (para los sistemas Microsoft® Windows®) o el archivo especial de dispositivo (para sistemas Linux) no sea idéntica a la letra de unidad en la consola de administración.

NOTA: Es posible que los medios virtuales no funcionen correctamente en los clientes con sistema operativo Windows que estén configurados con seguridad mejorada de Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador.

Desconexión de los medios virtuales

Haga clic en **Desconectar** para desconectar todas las imágenes y unidades virtuales de la estación de administración. Se desconectarán **todas** las imágenes y unidades virtuales y ya no estarán disponibles en el sistema administrado.

Conexión y desconexión del componente de medios virtuales

El componente de medios virtuales del DRAC 5 se basa en la tecnología USB y aprovecha las funciones Plug and Play de USB. El DRAC 5 agrega la opción de conectar y desconectar dispositivos virtuales del bus USB. Cuando los dispositivos se desconectan, el sistema operativo o BIOS no puede detectar ningún dispositivo conectado. Cuando los dispositivos virtuales se conectan, las unidades son visibles. A diferencia del DRAC 4, en donde las unidades sólo se podían activar y desactivar durante el siguiente inicio del sistema, los dispositivos virtuales del DRAC 5 se pueden conectar y desconectar en todo momento.

Los dispositivos virtuales se pueden conectar o desconectar por medio de un explorador de web, racadm local, racadm remota, Telnet y el puerto serie. Para configurar los medios virtuales por medio de un navegador Web, acceda a la página Medios y después a la página Configuración, donde puede cambiar la configuración y aplicarla. También puede especificar el Número de puerto de medios virtuales y el Número de puerto SSL de medios virtuales. Además, puede activar y desactivar la Memoria flash virtual y la función Iniciar una vez.

NOTA: Para activar la función Iniciar una vez, acceda a la configuración del BIOS y modifique manualmente el orden de inicio durante el reinicio del sistema.

Conexión automática de los medios virtuales

La versión 1.30 y las versiones posteriores del firmware del DRAC 5 admiten la función de conexión automática de medios virtuales. Cuando esta función se active, el DRAC 5 conectará automáticamente un dispositivo virtual al sistema únicamente cuando el dispositivo esté virtualizado (conectado) en un cliente admitido.

El DRAC 5 desconectará los dispositivos cuando la sesión de medios virtuales finalice.

Conexión, conexión automática y desconexión de los medios virtuales por medio del explorador de web

Para conectar el componente de medios virtuales, realice las siguientes acciones:

1. Haga clic en Sistema-> Medios-> Configuración
2. Seleccione la casilla Valor para Conectar medios virtuales
3. Haga clic en Aplicar cambios

Para desconectar el componente de medios virtuales, realice las siguientes acciones:

1. Haga clic en Sistema-> Medios-> Configuración
2. Deseleccione la casilla Valor para Conectar medios virtuales
3. Haga clic en Aplicar cambios

Conexión, conexión automática y desconexión de los medios virtuales por medio de RACADM

Para conectar la función de medios virtuales, abra una ventana del símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 1
```

Para desconectar el componente de medios virtuales, abra una ventana del símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 0
```

Para conectar automáticamente el componente de medios virtuales, abra una ventana del símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 2
```

Inicio desde los medios virtuales

En los sistemas admitidos, el BIOS de sistema permite iniciar desde unidades virtuales ópticas o virtuales de disco flexible. Durante la POST, ingrese a la ventana de configuración del BIOS y verifique que las unidades virtuales estén activadas y que aparezcan en el orden correcto.

Para cambiar la configuración del BIOS:

1. Inicie el sistema administrado.
2. Presione <F2> para ingresar a la ventana de configuración del BIOS.
3. Desplácese a la secuencia de inicio y presione <Entrar>.

   En la ventana emergente, aparece una lista de las unidades virtuales ópticas y de disco flexible virtuales con otros dispositivos normales de inicio.
4. Asegúrese que la unidad virtual esté activada y que aparezca como el primer dispositivo con medio iniciable. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.
5. Guarde los cambios y salga.

   El sistema administrado reinicia.

   El sistema administrado intenta iniciar desde un dispositivo iniciable basado en el orden de inicio. Si el dispositivo virtual está conectado y hay un medio iniciable presente, el sistema se iniciará desde el dispositivo virtual. De lo contrario, el sistema ignorará el dispositivo; como ocurriría con un dispositivo físico que no tiene medios iniciables.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas en terminar. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de los Medios virtuales puede tardar menos de 15 minutos en terminar. Consulte "Instalación del sistema operativo por medio de la VM-CLI" para obtener más información.

1. Verifique lo siguiente:
   - El CD de instalación de sistema operativo está insertado en la unidad de CD de la estación de administración.
   - La unidad de CD local está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección Inicio desde los medios virtuales para asegurarse que el BIOS está configurado para que inicie desde la unidad de CD a partir de la que se realiza la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

Utilización de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En los sistemas con Windows, las unidades de medios virtuales se montan automáticamente y se les asigna una letra de unidad.

La utilización de las unidades virtuales desde el interior de Windows es similar a la utilización de las unidades físicas. Cuando se conecta a los medios en una estación de administración, el medio está disponible en el sistema al hacer clic en la unidad y navegar el contenido.

Sistemas con Linux

En los sistemas con Linux, las unidades de medios virtuales no reciben una letra de unidad. En función del software que está instalado en el sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, móntelas manualmente.

Uso de la memoria flash virtual

El DRAC 5 tiene una memoria flash virtual permanente: 16 MB de memoria flash que reside en el sistema de archivos del DRAC 5 y que se puede usar como almacenamiento permanente al que el sistema tiene acceso. Cuando se activa, la memoria flash virtual se establece como tercer unidad virtual y aparece en el orden de inicio del BIOS, lo que permite que el usuario inicie desde la memoria flash virtual.

NOTA: Para iniciar desde la memoria flash virtual, la imagen de la misma debe ser una imagen iniciable.

A diferencia de la unidad de CD o de disco flexible que requiere una conexión de cliente externa o un dispositivo funcional en el sistema host, la implementación de la memoria flash virtual sólo necesita la función de memoria flash virtual permanente del DRAC 5. Los 16 MB de memoria flash aparecen como unidad USB extraíble sin formatear en el entorno de host.

Observe las siguientes directrices al implementar la memoria flash virtual:

- La conexión o desconexión de la memoria flash virtual ejecuta una reenumeración de USB, lo que conecta y desconecta todos los medios virtuales, respectivamente (por ejemplo, unidad de CD y unidad de disco flexible).
- Al activar o desactivar la memoria flash virtual, el estado de la conexión de la unidad de CD o de disco flexible de medios virtuales no cambia.

AVISO: Los procedimientos de desconexión y conexión interrumpen las operaciones activas de lectura y escritura de los medios virtuales.

Activación de la memoria flash virtual

Para activar la memoria flash virtual, abra una ventana del símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

Desactivación de la memoria flash virtual

Para desactivar la memoria flash virtual, abra una ventana del símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -gcfgRacVirtual -o cfgVirMediaKeyEnable 0
```

Almacenamiento de imágenes en una memoria flash virtual

La memoria flash virtual se puede formatear desde el host administrado. Si ejecuta un sistema operativo Windows, haga clic con el botón derecho del mouse en el icono de la unidad y seleccione **Formatear**. Si ejecuta Linux, las herramientas como format y fdisk permiten crear particiones y formatear el USB.

Antes de cargar una imagen desde el explorador de web del RAC en la memoria flash virtual, asegúrese que el archivo de imagen tenga un tamaño de entre 1,44 MB y 16 MB (inclusive) y que la memoria flash virtual esté desactivada. Después de descargar la imagen y de volver a activar la unidad de memoria flash virtual, el sistema y el BIOS reconocerán la memoria flash virtual.

Configuración de una memoria flash virtual iniciable

1. Inserte un disquete iniciable en la unidad correspondiente o inserte un CD iniciable en la unidad óptica.
2. Reinicie el sistema e inicie a partir de la unidad seleccionada.
3. Agregue una partición a la memoria flash virtual y active la partición.

   Utilice **fdisk** si la memoria flash virtual está emulando la unidad de disco duro. Si la memoria flash virtual está configurada como unidad B:, la memoria flash virtual emulará el disco flexible y no requerirá de particiones para configurarse como unidad iniciable.
4. Con el comando **format**, formatee la unidad con la opción /s para transferir los archivos de sistema a la memoria flash virtual.

   Por ejemplo,

   ```
   format /s x
   ```

   donde *x* es la letra de unidad que se asignó a la memoria flash virtual.
5. Apague el sistema y retire el disco flexible o CD iniciable de la unidad correspondiente.
6. Encienda el sistema y verifique que éste se inicie a partir de la memoria flash virtual hasta llegar al símbolo de sistema `C:\` o `A:\`.

Uso de la utilidad de interfaz de línea de comandos de los medios virtuales

La utilidad de interfaz de línea de comandos de los medios virtuales (VM-CLI) es una interfaz de línea de comandos que admite secuencias de comandos y ofrece funciones de medios virtuales de la estación de administración al DRAC 5 en el sistema remoto.

La utilidad VM-CLI proporciona las siguientes funciones:

- Admite varias sesiones activas de manera simultánea.

  NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.
- Dispositivos de medios extraíbles o archivos de imagen que son congruentes con los complementos de medios virtuales
- Terminación automática cuando se activa la opción de iniciar una vez del firmware del DRAC.
- Comunicaciones seguras con el DRAC 5 por medio de la Capa de conexión segura (SSL)

Antes de ejecutar la utilidad, compruebe que tiene privilegios de usuario de medios virtuales en el DRAC 5 del sistema remoto.

Si el sistema operativo admite los privilegios de administrador o un privilegio específico del sistema operativo o membresía a un grupo, también se necesitarán privilegios de administrador para ejecutar el comando de VM-CLI.

El administrador del sistema cliente controla los privilegios y grupos de usuarios, por consiguiente, controla cuáles usuarios pueden ejecutar la utilidad.

En el caso de los sistemas Windows, usted debe tener privilegios de usuario avanzado para ejecutar la utilidad VM-CLI.

En el caso de los sistemas Linux, usted debe acceder a la utilidad VM-CLI sin privilegios de administrador por medio del comando **sudo**. Este comando brinda un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos del usuario. Para agregar o editar usuarios en el grupo VM-CLI, el administrador utiliza el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de VM-CLI en el sistema remoto y pueden ejecutar la utilidad.

Instalación de la utilidad

La utilidad VM-CLI se encuentra en el DVD *Dell Systems Management Tools and Documentation*, que se incluye en el paquete de software Dell OpenManage System Management. Para instalar la utilidad, inserte el DVD *Dell Systems Management Tools and Documentation* en la unidad de DVD del sistema y siga las instrucciones que aparecen en la pantalla.

El DVD *Dell Systems Management Tools and Documentation* contiene los productos de software de administración de sistemas más recientes, incluso los diagnósticos, la administración de almacenamiento, el servicio de acceso remoto y la utilidad RACADM. Este DVD también contiene archivos readme (de lectura) con la información más reciente sobre los productos de software de administración de sistemas.

Además, el DVD *Dell Systems Management Tools and Documentation* incluye **vmdeploy**; una secuencia de comandos de ejemplo que ilustra el uso de las utilidades VM-CLI y RACADM para instalar software en varios sistemas remotos. Para obtener más información, consulte "Instalación del sistema operativo por medio de la VM-CLI".

Opciones de la línea de comandos

La interfaz de VM-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, la opción para especificar la dirección IP del DRAC 5 requiere la misma sintaxis en las utilidades RACADM y VM-CLI.

El formato del comando de VM-CLI es el siguiente:

`racvmcli` *`[parámetro] [opciones_de_shell_de_sistema_operativo]`*

NOTA: Necesita tener privilegios de **Administrador** para ejecutar el comando `racvmcli`.

En toda la sintaxis de la línea de comandos se distingue entre mayúsculas y minúsculas. Consulte "Parámetros de VM-CLI" para obtener más información.

Si el sistema remoto acepta los comandos y el DRAC 5 autoriza la conexión, el comando seguirá ejecutándose mientras no se presente uno de los siguientes casos:

- La conexión de VM-CLI termina por cualquier motivo.
- El proceso se termina manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, se puede usar el Administrador de tareas para terminar el proceso.

Parámetros de VM-CLI

Dirección IP del DRAC 5

`-r` *`<dirección_IP_del_RAC>[:<puerto_SSL_del_RAC>]`*

donde *`<dirección_IP_del_RAC>`* es una dirección IP válida y única o el nombre DDNS (sistema de nombres de dominio dinámico) (si se admite).

Este parámetro proporciona la dirección IP del DRAC 5 y el puerto SSL. La utilidad VM-CLI necesita esta información para establecer una conexión de medios virtuales con el DRAC 5 de destino. Si introduce un nombre de DDNS o una dirección IP no válida, aparecerá un mensaje de error y el comando terminará.

Si se omite *<puerto_SSL_del_RAC>*, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario, a menos que cambie el puerto SSL predeterminado del DRAC 5.

El nombre de usuario del DRAC 5

`-u` *`<nombre_de_usuario_del_DRAC>`*

Este parámetro proporciona el nombre de usuario del DRAC 5 que ejecutará los medios virtuales.

El <*nombre_de_usuario_del_DRAC*> debe tener los siguientes atributos:

- Nombre de usuario válido
- Permiso del usuario de los medios virtuales del DRAC

Si la autenticación del DRAC 5 falla, aparecerá un mensaje de error y el comando terminará.

Contraseña de usuario del DRAC

`-p` <*contraseña_de_usuario_del_DRAC*>

Este parámetro proporciona la contraseña para el usuario especificado del DRAC 5.

Si la autenticación del DRAC 5 falla, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de disco / disco flexible

`-f {`<*nombre_de_dispositivo*> | <*archivo_de_imagen*>`}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (en el caso de los sistemas Windows) o un nombre de archivo válido de dispositivo, que incluye el número de partición del sistema de archivo que se puede montar (en el caso de los sistemas Linux); y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

Este parámetro especifica el dispositivo o archivo que va a proporcionar el medio virtual de disco o disco flexible.

Por ejemplo, un archivo de imagen se especifica como:

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

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

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Configure el sistema operativo para proteger contra escritura una imagen de disco flexible que no desea que se sobrescriba.

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`-f /dev/sdb4 # 4ª partición en el dispositivo` /dev/sdb (sistema Linux)

Si el dispositivo tiene capacidad de protección contra escritura, utilice esta capacidad para garantizar que los medios virtuales no escribirán en el medio.

Además, omita este parámetro de la línea de comando si no está haciendo virtual un medio de disco flexible. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD / DVD

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde *<nombre_de_dispositivo>* es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo de CD/DVD válido (sistemas Linux) y *<archivo_de_imagen>* es el nombre y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o archivo que proporcionará el medio virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

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

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Windows)

`-c /dev/cdrom` (sistemas Linux)

Además, omita este parámetro de la línea de comando si no está haciendo virtual un medio de CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

`-v`

Este parámetro se usa para mostrar la versión de la utilidad VM-CLI Si no se proporcionan otras opciones además de interruptores, el comando terminará sin mensajes de error.

Mostrar la ayuda

`-h`

Este parámetro muestra un resumen de los parámetros de la utilidad VM-CLI. Si no se proporcionan otras opciones además de interruptores, el comando terminará sin errores.

Datos cifrados

-e

Cuando este parámetro se incluye en la línea de comandos, la utilidad VM-CLI utilizará un canal cifrado con SSL para transferir datos entre la estación de administración y el DRAC 5 en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifrará.

Opciones de shell de sistema operativo de VM-CLI

En la línea de comandos de VM-CLI se pueden usar las siguientes funciones de sistema operativo:

- stderr/stdout redirection: desvía los mensajes de salida impresos hacia un archivo.

  Por ejemplo, si se usa el carácter "mayor que" (>) seguido de un nombre de archivo, se sobrescribirá el archivo especificado con los mensajes de salida impresos de la utilidad VM-CLI.

  NOTA: La utilidad VM-CLI no lee en la entrada estándar (stdin). En consecuencia, la redirección de stdin no es necesaria.

- Ejecución en segundo plano: de manera predeterminada, la utilidad VM-CLI se ejecuta en el primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en el segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter et (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

Esta técnica es útil en los programas de secuencia de comandos, pues permite que la secuencia de comandos prosiga después de se inicia un nuevo proceso para el comando de VM-CLI (de lo contrario, la secuencia de comandos se bloquearía hasta que el programa de VM-CLI terminara). Cuando se inicien varias instancias de la VM-CLI de esta manera y se deban terminar una o varias instancias de comando manualmente, utilice las funciones específicas del sistema operativo para ver y finalizar procesos.

Códigos de retorno de la VM-CLI

0 = Sin errores

1 = No se puede conectar

2 = Error de línea de comandos de VM-CLI

3 = Se cerró la conexión del firmware del RAC

Cuando se presentan errores, también se envían mensajes de texto en inglés a la salida estándar de errores.

Instalación del sistema operativo por medio de la VM-CLI

La utilidad de interfaz de línea de comandos de los medios virtuales (VM-CLI) es una interfaz de línea de comandos y ofrece funciones de medios virtuales de la estación de administración al DRAC 5 en el sistema remoto. Por medio de la VM-CLI y los métodos de secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información sobre cómo integrar la utilidad VM-CLI en la red corporativa.

Antes de comenzar

Antes de usar la utilidad VM-CLI, compruebe que los sistemas remotos de destino y la red corporativa cumplan con los requisitos que aparecen en la secciones siguientes.

Requisitos de los sistemas remotos

- La tarjeta DRAC 5 está instalada en todos los sistemas remotos
- El dispositivo virtual en todos los sistemas remotos es el primer dispositivo en el orden de inicio del BIOS.

Integración personalizada de fábrica de Dell

Cuando pida el sistema Dell™ por medio de las opciones de la Integración personalizada de fábrica (CFI) de Dell, Dell puede preconfigurar el sistema con una tarjeta DRAC 5 que incluya un nombre DDNS y un BIOS preconfigurado de sistema que esté habilitado para medios virtuales. Con esta configuración, el sistema está listo para iniciar a partir de los dispositivos de medios virtuales del mismo cuando se instale en la red corporativa.

Para obtener más información, consulte el sitio web de Dell en **www.dell.com**.

Requisitos de red

Debe tener un recurso compartido de red que contenga:

- Los archivos de sistema operativo
- Los controladores necesarios
- Los archivos de imagen de inicio del sistema operativo

El archivo de imagen debe ser una imagen de disco flexible 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, compruebe que el sistema compatible puede iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba con la interfaz web de usuario del DRAC 5 y después reinicie el sistema.

Las secciones siguientes contienen información específica para la creación de archivos de imagen para los sistemas Linux y Windows.

Creación de un archivo de imagen para los sistemas Linux

Use la utilidad Data Duplicator para crear un archivo de imagen iniciable para el sistema Linux.

Para ejecutar la utilidad, abra una ventana del símbolo del sistema y escriba lo siguiente:

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

Por ejemplo,

```
dd if=/dev/fd0 of=myfloppy.img
```

Creación de un archivo de imagen para los sistemas Windows

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

Preparación para la instalación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que la estación de administración pueda acceder.
2. Copie los archivos de sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen iniciable preconfigurado para instalación, cree el archivo. Incluya los programas y/o secuencias de comando que se utilizan para los procedimientos de instalación del sistema operativo

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

   Cuando cree el archivo de imagen, asegúrese de lo siguiente:

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

- Realice uno de los procedimientos siguientes:
  - Integre RACADM y la interfaz de línea de comandos de medios virtuales (VM-CLI) en la aplicación existente de instalación del sistema operativo. Utilice la secuencia de comandos de instalación de ejemplo como guía al momento de integrar las utilidades del DRAC 5 en la aplicación existente de instalación de sistema operativo.
  - Utilice la secuencia de comandos **vmdeploy** existente para instalar el sistema operativo.

Instalación del sistema operativo

Use la utilidad VM-CLI y la secuencia de comandos vmdeploy que se incluye con la utilidad para instalar el sistema operativo en los sistemas remotos.

Antes de comenzar, revise la secuencia de comandos vmdeploy de ejemplo que se incluye con la utilidad VM-CLI. La secuencia de comandos ofrece los requisitos detallados para instalar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento es una descripción general de la instalación del sistema operativo en los sistemas remotos de destino.

1. Identifique los sistemas remotos en los que se van a realizar las instalaciones.
2. Registre los nombres y las direcciones IP de los DRAC 5 de los sistemas remotos de destino.
3. Ejecute el siguiente procedimiento en cada sistema remoto de destino:
   a. Configure un proceso de VM-CLI que incluya los siguientes parámetros para el sistema de destino:
      - Dirección IP o nombre DDNS del DRAC 5
      - Nombre del archivo de imagen iniciable de instalación
      - Nombre de usuario del DRAC 5
      - Contraseña de usuario del DRAC 5
   b. Con RACADM, establezca la opción **iniciar una vez** del DRAC 5 de destino.
   c. Reinicie el sistema de DRAC 5 por medio de RACADM.

Preguntas más frecuentes

Algunas veces, he notado que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?

Cuando se agota el tiempo de espera de la red, el firmware del DRAC 5 cierra la conexión, lo que desconecta el vínculo entre el servidor y la unidad virtual. Para restablecer la conexión con el disco virtual, use la función de Medios virtuales.

¿Qué sistemas operativos son compatibles con el DRAC 5?

Consulte la Matriz de compatibilidad de software de los sistemas Dell que se encuentra en el sitio web de asistencia de Dell en support.dell.com para ver una lista de los sistemas operativos compatibles.

¿Qué exploradores de web son compatibles con el DRAC 5?

Consulte la *Matriz de compatibilidad de software de los sistemas Dell* que se encuentra en el sitio web de asistencia de Dell en **support.dell.com** para ver una lista de los exploradores de web que son compatibles.

¿Por qué a veces se pierde mi conexión de cliente?

- Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD en la unidad de CD del sistema cliente, en nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión cuando el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior.
- Cuando se agota el tiempo de espera de la red, el firmware del DRAC 5 cierra la conexión, lo que desconecta el vínculo entre el servidor y la unidad virtual. Para restablecer la conexión con el disco virtual, use la función de Medios virtuales.

¿Qué debo hacer si Windows 2000 con Service Pack 4 no se instala correctamente?

Si utiliza los medios virtuales y el CD del sistema operativo Windows 2000 para instalar Windows 2000 con Service Pack 4, es posible que el sistema pierda momentáneamente la conexión con la unidad de CD durante el procedimiento de instalación y el sistema operativo puede no instalarse correctamente. Para resolver este problema, descargue el archivo usbstor.sys del sitio web de asistencia técnica de Microsoft en **support.microsoft.com** y ejecute el programa únicamente en los sistemas que presenten este problema. Para obtener más información, consulte el artículo 823086 de Microsoft Knowledge Base.

¿Por qué no puedo instalar Windows 2000 de manera local o remota?

Este problema normalmente ocurre cuando la memoria flash virtual está activada y no tiene una imagen válida, por ejemplo, cuando la memoria flash virtual contiene una imagen dañada o aleatoria, es posible que no se pueda instalar Windows 2000 de manera local o aleatoria. Para resolver este problema, instale una imagen válida en la memoria flash virtual o desactive la memoria flash virtual si no la va a utilizar durante el procedimiento de instalación.

¿Por qué se cierra la conexión de medios virtuales cuando está configurada en el modo de NIC compartido?

La instalación de los controladores de red y de chipset hace que la conexión de medios virtuales se cierre cuando está configurada en el modo de NIC compartido. La instalación de los controladores de red o de chipset hace que el LOM se restablezca, lo que, a su vez, hace que los paquetes de red agoten el tiempo de espera y que la conexión de medios virtuales agote el tiempo de espera y se cierre. Para evitar este problema, copie los controladores de la unidad virtual a la unidad de disco duro local del servidor. Para evitar que una conexión de medios virtuales que se cerró interfiera con el procedimiento de instalación del controlador, inicie la instalación del controlador directamente del servidor.

La instalación del sistema operativo Windows parece tardar demasiado. ¿Por qué?

Si instala el sistema operativo Windows por medio del DVD *Dell Systems Management Tools and Documentation* y la conexión de red es lenta, es posible que el procedimiento de instalación requiera más tiempo para acceder a la interfaz Web del DRAC 5 debido a la latencia de la red. Mientras la ventana de instalación no indique el progreso de la instalación, significa que el procedimiento de instalación está en progreso.

Veo el contenido de una unidad de disco flexible o memoria USB. Si trato de establecer una conexión de medios virtuales con la misma unidad, recibo un mensaje de error de conexión y se me pide que vuelva a intentarlo. ¿Por qué?

No se permite el acceso simultáneo a las unidades de disco flexible virtual. Cierre la aplicación que se utiliza para ver el contenido de la unidad antes de que intente hacer virtual la unidad.

¿Cómo configuro mi dispositivo virtual como dispositivo iniciable?

En el sistema administrado, acceda a la configuración del BIOS y diríjase al menú de inicio. Localice el CD virtual, el disco flexible virtual o la memoria flash virtual y cambie el orden de dispositivo de inicio según corresponda. Por ejemplo, para iniciar a partir de una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.

¿A partir de qué tipos de medios puedo iniciar el sistema?

El DRAC 5 permite iniciar el sistema desde los siguientes tipos de medios iniciables:

- Medios de CDROM/DVD de datos
- Imagen ISO 9660
- Imagen de disco flexible o disco flexible de 1,44 pulgadas
- Memoria flash virtual incorporada de DRAC 5
- Una memoria USB a la que el sistema operativo reconoce como disco extraíble
- Una imagen de memoria USB

¿Cómo puedo hacer que mi memoria USB sea iniciable?

Sólo las memorias USB con DOS de Windows 98 se pueden iniciar a partir del disco flexible virtual. Para configurar su propia memoria USB iniciable, inicie desde un disco de arranque de Windows 98 y copie los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, desde una vetana del símbolo del sistema DOS, escriba el comando siguiente:

```
sys a: x: /s
```

donde "x:" es la memoria USB que desea hacer iniciable.

También puede usar la utilidad de inicio de Dell para crear una memoria USB iniciable. Esta utilidad sólo es compatible con las memorias USB de marca Dell. Para descargar la utilidad, abra el explorador de web compatible, navegue hasta el sitio web de asistencia técnica de Dell en support.dell.com y busque "R122672.exe".

¿Necesito privilegios de administrador para instalar el complemento ActiveX?

Debe tener privilegios de administrador o de usuario avanzado en los sistemas operativos Windows para instalar el complemento de medios virtuales.

¿Qué privilegios necesito para instalar y usar el complemento de medios virtuales en una estación de administración Red Hat Linux?

Debe tener privilegios de Escritura en el árbol de directorio del explorador para instalar el complemento de medios virtuales correctamente.

No puedo encontrar mi dispositivo de disco flexible virtual en un sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux. Mis medios virtuales están conectados y estoy conectado a mi disco flexible remoto. ¿Qué debo hacer?

Algunas versiones de Linux no montan automáticamente la unidad de disco flexible virtual y la unidad de CD virtual de manera similar. Para montar la unidad de disco flexible virtual, localice el nodo de dispositivo que Linux asigna a la unidad de disco flexible virtual. Ejecute los siguientes pasos para encontrar y montar correctamente la unidad de disco flexible virtual:

1. Abra una ventana del símbolo del sistema de Linux y ejecute el siguiente comando:

   grep "Virtual Floppy" ("Disco flexible virtual") /var/log/messages

2. Localice la última anotación de dicho mensaje y anote la hora.
3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando:

   grep "hh:mm:ss" /var/log/messages
   donde:

   hh:mm:ss es la hora del mensaje que el comando grep informó en el paso 1.

4. En el paso 3, lea el resultado del comando grep y localice el nombre de dispositivo que se asignó a "Disco flexible virtual de Dell"
5. Asegúrese que está conectado a la unidad de disco flexible virtual.
6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando:

   mount /dev/sdx /mnt/floppy

   donde:

   /dev/sdx es el nombre de dispositivo que se encontró en el paso 4

   /mnt/floppy es el punto de montaje.

¿Qué tipos de sistema de archivos se admiten en mi unidad de disco flexible virtual o en mi memoria flash virtual?

Su unidad de disco flexible virtual o memoria flash virtual admite sistemas de archivos FAT16 o FAT32.

Cuando ejecuté una actualización de firmware de manera remota con la interfaz basada en web del DRAC 5, mis unidades virtuales fueron eliminadas. ¿Por qué?

Las actualizaciones de firmware hacen que el DRAC 5 se restablezca, cierre la conexión remota y desmonte las unidades virtuales. Las unidades volverán a aparecer cuando termine el restablecimiento del DRAC.

Cuando activo y desactivo la memoria flash virtual, he notado que todas mis unidades virtuales desaparecen y vuelven a aparecer. ¿Por qué?

La desactivación o activación de la memoria flash virtual hace que el USB se restablezca y ocasiona que todas las unidades virtuales se desconecten y se vuelvan a conectar al bus USB.

¿Cómo puedo instalar un explorador de web en mi estación de administración que tiene un sistema de archivos de sólo lectura?

Si está ejecutando Linux y la estación de administración tiene un sistema de archivos de sólo lectura, se puede instalar un explorador en un sistema cliente sin requerir una conexión al DRAC 5. Si utiliza el paquete de instalación nativo del complemento, el explorador se puede instalar manualmente durante la fase de configuración del cliente.

AVISO: En un entorno de cliente de sólo lectura, si el firmware del DRAC 5 se actualiza con una versión más reciente del complemento, el complemento VM instalado no funcionará. Esto se debe a que las funciones del complemento anterior no tienen permiso de funcionar cuando el firmware contiene una versión más reciente del complemento. En este caso, se pedirá la instalación de complemento en el cliente. Como el sistema de archivos es de sólo lectura, la instalación fallará y las funciones del complemento no estarán disponibles.

Para obtener el paquete de instalación del complemento:

1. Inicie sesión en un DRAC 5 existente
2. Cambie el URL en la barra de dirección del explorador, de:

```
https://<IP_del_RAC>/cgi-bin/webcgi/main
```

a:

```
https://<IP_del_RAC>/plugins/ # Be sure to include the trailing slash. (Asegúrese de incluir la última diagonal.)
```

3. Localice los dos subdirectorios, vm y vkvm. Desplácese hacia el subdirectorio correspondiente, haga clic con el botón derecho del mouse en el archivo rac5XXX.xpi y seleccione Guardar destino como....
4. Elija una ubicación para guardar el archivo del paquete de instalación del complemento.

Para instalar el paquete de instalación del complemento:

1. Copie el paquete de instalación en el recurso compartido del sistema de archivos nativo del cliente que esté accesible para el cliente.
2. Abra una instancia del explorador en el sistema cliente.
3. Introduzca la ruta de acceso del archivo del paquete de instalación del complemento en la barra de dirección del explorador. Por ejemplo,

```
file:///tmp/rac5vm.xpi
```

4. El explorador guiará al usuario a través de la instalación del complemento.

Una vez instalado, el explorador no volverá a solicitar la instalación del complemento, siempre y cuando el firmware del DRAC 5 de destino no contenga una versión más reciente de ese complemento.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de las funciones de seguridad

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

El DRAC 5 ofrece las siguientes funciones de seguridad:

- Opciones de seguridad avanzada para el administrador del DRAC:
  - La opción de desactivación de la redirección de consola permite que el usuario *local* del sistema desactive la redirección de consola por medio de la función de redirección de consola del DRAC 5.
  - Las funciones de desactivación de la configuración local permiten que el administrador del DRAC *remoto* desactive de manera selectiva la capacidad de configurar el DRAC 5 a partir de:
    - La ROM de opción de la POST del BIOS
    - El sistema operativo por medio de racadm local y las utilidades de Dell OpenManage™ Server Administrator
- La operación de la interfaz basada en web y la CLI de RACADM, que admite el cifrado SSL de 128 bits y el cifrado SSL de 40 bits (para los países en los que no se acepta el cifrado de 128 bits)

  NOTA: Telnet no admite el cifrado SSL.

- Configuración del tiempo de espera de sesión (en segundos) mediante la interfaz basada en web o la CLI de RACADM
- Puertos IP que se pueden configurar (en los casos correspondientes)
- Secure Shell (SSH), que utiliza una capa cifrada de transporte para brindar una mayor seguridad.
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.
- Rango limitado de direcciones IP para clientes que se conectan al DRAC 5

Opciones de seguridad para el administrador del DRAC

Desactivación de la configuración local del DRAC 5

Los administradores pueden desactivar la configuración local por medio de la interfaz gráfica de usuario del DRAC 5 al seleccionar **Acceso remoto**→ **Configuración**→ **Servicios**. Cuando se selecciona la casilla **Desactivar la configuración local del DRAC por medio de la ROM de opción**, la utilidad de configuración de acceso remoto —a la cual se accede al presionar Ctrl+E durante el inicio del sistema— funciona en modo de sólo lectura, lo que evita que los usuarios locales puedan configurar el dispositivo. Cuando el administrador selecciona la casilla **Desactivar la configuración local del DRAC por medio de RACADM**, los usuarios locales no pueden configurar el DRAC 5 por medio de la utilidad racadm ni mediante Dell OpenManage Server Administrator, pero aún pueden leer los valores de la configuración.

Los administradores pueden activar una de estas opciones al mismo tiempo o ambas. Además de activarlas por medio de la interfaz gráfica de usuario, los administradores también pueden utilizar los comandos locales de racadm.

Desactivación de la configuración local durante el reinicio del sistema

Esta función desactiva la capacidad que tiene el usuario del sistema administrado de configurar el DRAC 5 durante el reinicio del sistema.

```
racadm config -g cfgRacTune -o
```

```
cfgRacTuneCtrlEConfigDisable 1
```

NOTA: Esta opción sólo es compatible con la utilidad Remote Access Configuration Utility versión 1.13 y posteriores. Para actualizarse con esta versión, actualice el BIOS por medio del paquete de actualización del BIOS que se encuentra en el DVD *Dell Server Updates* o en el sitio web de asistencia técnica de Dell en **support.dell.com**.

Desactivación de la configuración local a partir de racadm local

Esta función desactiva la capacidad del usuario del sistema administrado de configurar el DRAC 5 por medio de las utilidades de racadm local o de Dell OpenManage Server Administrator.

```
racadm config -g cfgRacTune -o cfgRacTuneLocalConfigDisable 1
```

AVISO: Estas funciones limitan en gran medida la capacidad del usuario local para configurar el DRAC 5 desde el sistema local, lo que incluye el restablecimiento de la configuración predeterminada. Dell recomienda que se utilicen estas funciones a discreción y se debe desactivar sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión.

NOTA: Para obtener más información, consulte del documento técnico *Disabling Local Configuration and Remote Virtual KVM in the DRAC (Desactivación de la configuración local y el KVM virtual remoto en el DRAC)* en el sitio web de asistencia técnica de Dell en **support.dell.com**.

Aunque los administradores pueden establecer las opciones de configuración local por medio de los comandos de racadm local, por motivos de seguridad sólo pueden restablecerlos a partir de una interfaz de línea de comandos o una interfaz gráfica del DRAC 5 fuera de banda. La opción `cfgRacTuneLocalConfigDisable` se aplica una vez que la autoprueba de encendido del sistema ha terminado y el sistema ha iniciado por completo el entorno del sistema operativo. El sistema operativo puede ser un sistema tal como Microsoft® Windows Server® o Enterprise Linux que pueda ejecutar localmente comandos de racadm, o bien un sistema operativo de uso limitado tal como el Entorno de Preinstalación de Microsoft Windows® o vmlinux, utilizado para ejecutar los comandos de racadm locales de Dell OpenManage Deployment Toolkit.

Hay varias situaciones que pueden requerir que los administradores desactiven la configuración local. Por ejemplo, en un centro de datos con varios administradores para servidores y dispositivos de acceso remoto, es posible que los responsables de mantener las pilas de software de servidor no necesiten tener acceso a los dispositivos de acceso remoto. Asimismo, los técnicos pueden tener acceso físico a los servidores durante mantenimiento de rutina de sistemas —durante el cual pueden reiniciar los sistemas y acceder al BIOS protegido con contraseña— pero no deben tener la facultad de configurar los dispositivos de acceso remoto. En situaciones de este tipo, es recomendable que los administradores de dispositivos de acceso remoto desactiven la configuración local.

Los administradores deben tener presente que debido a que la desactivación de la configuración local limita en gran medida los privilegios de configuración local —incluso la capacidad de restablecer la configuración predeterminada del DRAC 5— sólo deben utilizar estas opciones cuando sea necesario y normalmente deberán desactivar sólo una interfaz a la vez para evitar la pérdida de todos los privilegios de inicio de sesión. Por ejemplo, si los administradores han deshabilitado a todos los usuarios locales del DRAC 5 y sólo permiten que los usuarios del servicio de directorio Microsoft Active Directory® inicien sesión en el DRAC 5, y posteriormente falla la infraestructura de autenticación de Active Directory, es posible que los administradores no puedan iniciar sesión. Asimismo, si los administradores han desactivado toda la configuración local e incorporan un DRAC 5 con una dirección IP estática a una red que ya incluye un servidor de Protocolo de configuración de host dinámica (DHCP), y éste luego asigna la dirección IP del DRAC 5 a otro dispositivo de la red, debido al conflicto resultante existe la posibilidad de que se desactive la conectividad fuera de banda del DRAC, lo que obliga a los administradores a restablecer la configuración predeterminada del firmware por medio de una conexión serie.

Desactivación del KVM virtual remoto del DRAC 5

Los administradores pueden desactivar de manera selectiva el VKM virtual del DRAC 5, lo que brinda un mecanismo seguro y flexible para que el usuario local trabaje en el sistema sin que alguien más vea las acciones del usuario a través de la redirección de consola. El uso de esta función requiere la instalación de software de nodo administrado del DRAC en el servidor. Los administradores pueden desactivar el vKVM remoto con el siguiente comando:

```
racadm LocalConRedirDisable 1
```

El comando LocalConRedirDisable desactiva las ventanas de sesión vKVM remota existentes cuando se ejecuta con el argumento 1

Para ayudar a evitar que el usuario remoto anule la configuración del usuario local, este comando sólo está disponible para racadm local. Los administradores pueden usar este comando en los sistemas operativos que admiten racadm local, incluso en Microsoft Windows Server 2003 y SUSE Linux Enterprise Server 10. Como los efectos de este comando continúan después de reinicios del sistema, los administradores deben revertirlo específicamente para reactivar el vKVM remoto. Pueden hacer esto con el argumento 0:

```
racadm LocalConRedirDisable 0
```

Hay varias situaciones que pueden requerir la desactivación del vKVM remoto del DRAC 5. Por ejemplo, es posible que los administradores no deseen que un

usuario del DRAC 5 remoto vea la configuración del BIOS que han establecido en un sistema, en tal caso, pueden desactivar el vKVM remoto durante la POST del sistema por medio del comando `LocalConRedirDisable`. Si también desean aumentar la seguridad a través de la desactivación automática del vKVM remoto cada vez que un administrador inicie sesión en el sistema, lo pueden hacer mediante la ejecución del comando `LocalConRedirDisable` en las secuencias de comandos de inicio de sesión del usuario.

NOTA: Para obtener más información, consulte del documento técnico *Disabling Local Configuration and Remote Virtual KVM in the DRAC (Desactivación de la configuración local y el KVM virtual remoto en el DRAC)* en el sitio web de asistencia técnica de Dell en **support.dell.com**.

Para obtener más información sobre las secuencias de comando de inicio de sesión, consulte **technet2.microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx.**

Cómo hacer que las comunicaciones del DRAC 5 sean seguras por medio de certificados digitales y de SSL

Este apartado contiene información sobre las siguientes características de seguridad de datos que están incorporadas en el DRAC 5:

- "Capa de conexión segura (SSL)"
- "Solicitud de firma de certificado (CSR)"
- "Acceso al menú principal de SSL"
- "Generación de una nueva solicitud de firma de certificado"
- "Carga de un certificado de servidor"
- "Carga de un certificado de servidor"

Capa de conexión segura (SSL)

El DRAC incluye un servidor web que está configurado para usar el protocolo de seguridad SSL que es el estándar industrial para transferir datos cifrados a través de la Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas y es una técnica ampliamente aceptada para ofrecer comunicación cifrada y autenticada entre los clientes y servidores a fin de evitar intercepción furtiva a la información de la red.

Un sistema habilitado para SSL:

- Se autentica a sí mismo en un cliente habilitado para SSL
- Permite que el cliente se autentique a sí mismo en el servidor
- Permite que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado brinda una protección de datos de alto nivel. El DRAC utiliza el cifrado SSL estándar de 128 bits, la forma más segura de cifrado que está normalmente disponible en los exploradores de Internet en Norteamérica.

El servidor web del DRAC incluye un certificado digital SSL autofirmado de Dell (Identificación de servidor). Para asegurar una mayor seguridad en la Internet, reemplace el certificado SSL de servidor web mediante el envío de una nueva solicitud al DRAC para generar una nueva solicitud de firma de certificado (CSR).

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (CA) para obtener un certificado de servidor seguro. Los certificados de servidor seguro protegen la identidad de un sistema remoto y garantizan que otros usuarios no puedan ver o cambiar la información que se intercambia con dicho sistema. Para garantizar la seguridad del DRAC, se recomienda enfáticamente que se genere una CSR, se envíe a una autoridad de certificados y se cargue el certificado devuelto por la autoridad de certificados.

Una autoridad emisora de certificados es una entidad comercial que está reconocida por la industria de la tecnología informática por cumplir estándares altos de revisión confiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Después de recibir la solicitud CSR, la autoridad de certificados (CA) revisa y verifica la información que contiene. Si el candidato cumple los estándares de seguridad de la autoridad de certificados, ésta emite un certificado al candidato que lo identifica de forma exclusiva para transacciones a través de redes y en Internet.

Después de que la CA aprueba la CSR y le envía un certificado, se debe cargar el certificado en el firmware del DRAC. La información de la CSR almacenada en el firmware del DRAC debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **SSL**.

Use las opciones de la página **Menú principal de SSL** (consulte la Tabla 11-1) para generar una CSR para enviarla a una autoridad de certificados. La información de la CSR se almacena en el firmware del DRAC 5. La Tabla 11-2 describe los botones disponibles en la página **Menú principal de SSL**.

Tabla 11-1. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	Haga clic en **Siguiente** para abrir la página **Generación de una solicitud de firma de certificado**, que permite generar una CSR para su envío a una CA para solicitar un certificado web seguro. **AVISO:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la CA acepte la CSR, la CSR que está en el firmware debe coincidir con el certificado que la CA devuelve.
Cargar certificado de servidor	Haga clic en **Siguiente** para cargar un certificado existente sobre el que su empresa tiene derechos y que utiliza para controlar el acceso al DRAC 5. **AVISO:** El DRAC 5 sólo acepta certificados codificados con X509, Base 64. No se aceptan los certificados codificados con DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su DRAC 5.
Ver el certificado de servidor	Haga clic en **Siguiente** para ver un certificado de servidor existente.

Tabla 11-2. Botones del menú principal de SSL

Botón	Descripción
Imprimir	Imprime la página **Menú principal de SSL**.
Next	Avanza a la página siguiente.

Generación de una nueva solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la autoridad de certificados (CA) acepte la CSR, la CSR que está en el firmware debe coincidir con el certificado que la CA devuelve. De lo contrario, el DRAC 5 no cargará 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)**, escriba un valor para cada atributo de la CSR.

   La Tabla 11-3 describe las opciones de la página **Generar solicitud de firma de certificado (CSR)**.
3. Haga clic en **Generar** para guardar o ver la CSR.
4. Haga clic en el botón de la página **Generar solicitud de firma de certificado (CSR)** para continuar. La Tabla 11-4 describe los botones que están disponibles en la página **Generar solicitud de firma de certificado (CSR)**.

Tabla 11-3. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, www.empresaxyz.com). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Grupo de empresa). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Monterrey). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo o algún otro carácter.
Nombre del estado:	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Nuevo León). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación. Utilice el menú desplegable para seleccionar el país.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Puede escribir la dirección de correo electrónico de su empresa o cualquier dirección de correo electrónico que desee tener asociada con la CSR. Este campo es opcional.

Tabla 11-4. Botones de la página Generar solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime la página **Generar solicitud de firma de certificado (CSR)**.
Volver al menú principal de seguridad	Regresa a la página **Menú principal de SSL**.
Generar	Genera una CSR.

Carga de un certificado de servidor

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

   Aparecerá la página **Carga de certificado**.

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

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

3. Haga clic en **Aplicar**.
4. Haga clic en el botón correspondiente de la página para continuar.

Cómo ver un certificado de servidor

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

   La Tabla 11-5 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Haga clic en el botón correspondiente de la página **Ver certificado de servidor** para continuar.

Tabla 11-5. Información de certificados

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

Uso de Secure Shell (SSH)

Sólo se admiten cuatro sesiones SSH a la vez. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se decribe en "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5".

Usted puede activar el SSH en el DRAC 5 con el comando:

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

Puede cambiar el puerto SSH con el comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>
```

Para obtener más información sobre las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5".

La implementación de SSH del DRAC 5 admite varios esquemas de criptografía, según se muestra en la Tabla 11-6.

Tabla 11-6. Esquemas de criptografía

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

NOTA: No se admite SSHv1.

Configuración de servicios

NOTA: Para modificar esta configuración, debe tener permiso para **Configurar el DRAC 5**. Además, la utilidad de línea de comandos de RACADM sólo se puede activar si el usuario ha iniciado sesión como **root**.

1. Amplíe el árbol de **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Servicios**.
3. Configure los servicios siguientes según sea necesario:
   - Configuración local (Tabla 11-7)
   - Servidor web (Tabla 11-8)
   - SSH (Tabla 11-9)
   - Telnet (Tabla 11-10)
   - RACADM remota (Tabla 11-11)
   - Agente SNMP (Tabla 11-12)
   - Agente de recuperación automatizada del sistema (Tabla 11-13)

   Utilice el Agente de recuperación automatizada del sistema para activar la función de Pantalla de último bloqueo del DRAC 5.

   NOTA: Para que la opción Pantalla de último bloqueo funcione en el DRAC 5, Server Administrator debe estar instalado con la función Recuperación automática activada mediante el establecimiento de Acción en: Reiniciar sistema, Apagar sistema o Realizar ciclo de encendido del sistema.
4. Haga clic en **Aplicar cambios**.
5. Para continuar, haga clic en el botón adecuado de la página **Servicios**. Consulte el apartado Tabla 11-14.

Tabla 11-7. Valores de configuración local

Valor	Descripción
Desactivar la configuración local del DRAC	Desactiva la configuración local del DRAC 5 por medio de la ROM de opción. La ROM de opción le pedirá que

por medio de la ROM de opción	introduzca el módulo de configuración con la combinación de teclas <Ctrl+E> durante el reinicio del sistema.
Desactivar la configuración local del DRAC por medio de RACADM	Desactiva la configuración local del DRAC 5 por medio de RACADM.

Tabla 11-8. Configuración del servidor web

Valor	Descripción
Activado	Activa o desactiva el servidor web. Seleccionada=activado; deseleccionada=desactivado.
N.° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **N.° máx. de sesiones**.
Tiempo de espera	El tiempo en segundos que se permite que la conexión permanezca abierta sin actividad. La sesión se cierra cuando se alcanza el tiempo de espera. Los cambios al valor de tiempo de espera no afectan la sesión actual. Cuando cambie el valor del tiempo de espera, deberá cerrar sesión e iniciar sesión nuevamente para que el nuevo valor surta efecto. El rango del tiempo de espera es de 60 a 1920.
Número de puerto de HTTP	El puerto que el DRAC utiliza para detectar una conexión de servidor. El valor predeterminado es **80**.
Número de puerto de HTTPS	El puerto que el DRAC utiliza para detectar una conexión de servidor. El valor predeterminado es **443**.

Tabla 11-9. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Seleccionada=activado; deseleccionada=desactivado.
N.° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Se admiten hasta cuatro sesiones.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **N.° máx. de sesiones**.
Tiempo de espera	El tiempo de espera sin actividad de Secure Shell, en segundos. Rango = 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 que el DRAC utiliza para detectar una conexión de servidor. El valor predeterminado es 22.

Tabla 11-10. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Seleccionada=activado; deseleccionada=desactivado.
N.° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Se admiten hasta cuatro sesiones.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **N.° máx. de sesiones**.
Tiempo de espera	El tiempo de espera sin actividad de Secure Shell, en segundos. Rango = 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 que el DRAC utiliza para detectar una conexión de servidor. El valor predeterminado es 23.

Tabla 11-11. Configuración de RACADM remota

Valor	Descripción
Activado	Activa o desactiva RACADM remota. Seleccionada=activado; deseleccionada=desactivado.
N.° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Se admiten hasta cuatro sesiones.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **N.° máx. de sesiones**.

Tabla 11-12. Configuración del agente SNMP

Valor	Descripción
Activado	Activa o desactiva el agente SNMP. Seleccionada=activado; deseleccionada=desactivado.
Nombre de comunidad	El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. El valor predeterminado es **public**.

Tabla 11-13. Configuración del agente de recuperación automatizada del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automatizada del sistema.

Tabla 11-14. Botones de la página Servicios

Botón	Descripción
Imprimir	Imprime la página **Servicios**.
Actualizar	Actualiza la página **Servicios**.
Aplicar cambios	Aplica los valores de la página **Servicios**.

Activación de las opciones adicionales de seguridad del DRAC 5

Para evitar accesos no autorizados al sistema remoto, el DRAC 5 tiene las siguientes funciones:

- Filtrado de direcciones IP (IpRange): define un rango específico de direcciones IP que pueden acceder al DRAC 5.
- Bloqueo de direcciones IP: limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica

Estas funciones están desactivadas en la configuración predeterminada del DRAC 5. Utilice el subcomando siguiente o la interfaz basada en web para activar estas funciones:

```
racadm config -g cfgRacTuning -o <nombre_de_objeto> <valor>
```

Además, use estas funciones en combinación con los valores correspondientes de tiempo de espera de la sesión y un plan de seguridad definido para la red.

Los apartados siguientes contienen información adicional sobre estas funciones.

Filtrado de IP (IpRange)

El filtrado de direcciones IP (o *Comprobación de IpRange*) permite que sólo tengan acceso al DRAC 5 los clientes o estaciones de trabajo cuyas direcciones IP están dentro de un rango que el usuario especifica. Los demás inicios de sesión se rechazan.

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de **cfgRacTuning**:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propiedad **cfgRacTuneIpRangeMask** se aplica a la dirección IP entrante y a las propiedades **cfgRacTuneIpRangeAddr**. Si los resultados de ambas propiedades son idénticos, a la solicitud de inicio de sesión entrante se le concederá acceso al DRAC 5. Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión procederá si el valor de la siguiente expresión es igual a cero:

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

donde & es el operador Y a nivel de bits de las cantidades y ^ es el operador O exclusivo a nivel de bits.

Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5" para ver una lista completa de las propiedades de **cfgRacTune**.

Tabla 11-15. Propiedades del filtrado de direcciones IP (IpRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación de rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Esta propiedad es una comparación con operador Y a nivel de bits con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. A todas las direcciones IP que contengan este patrón de bits en los bits superiores se les permitirá establecer una sesión en el DRAC 5. Los inicios de sesión provenientes de direcciones IP que estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que un rango de direcciones de 192.168.1.0 a 192.168.1.255 puedan establecer una sesión en el DRAC 5.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en forma de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior.

Activación del filtrado de IP

A continuación, se muestra un comando de ejemplo para la configuración del filtrado de IP.

Consulte "Uso de RACADM de manera remota" para obtener más información sobre RACADM y los comandos RACADM.

NOTA: Los siguientes comandos RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57)

Para restringir el inicio de sesión a una sola dirección IP (por ejemplo, 192.168.0.57), utilice toda la máscara, según se muestra a continuación.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Directrices para el filtrado de IP

Utilice las directrices a continuación cuando active el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Use la dirección base de rango que prefiera como el valor de **cfgRacTuneIpRangeAddr**. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits de orden inferior donde hay ceros en la máscara.

Bloqueo de IP

El bloqueo de IP determina de manera dinámica cuando se presenten intentos fallidos excesivos de inicio de sesión provenientes de una dirección IP específica y bloquea (o evita) que la dirección inicie sesión en el DRAC 5 durante un periodo predefinido.

El parámetro de bloqueo de IP utiliza las funciones del grupo **cfgRacTuning** que incluyen:

- El número de intentos fallidos de inicio de sesión que se permiten
- El periodo en segundos dentro del que se deben presentar estos intentos fallidos
- La cantidad de tiempo en segundos que se impedirá que la dirección IP "responsable" establezca una sesión después de haber superado el número total permisible de intentos fallidos

Conforme se acumulan los intentos fallidos de inicio de sesión provenientes de una dirección IP específica, estos se "añejan" por medio de un contador interno. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: Identificación de intercambio de SSH: Connection closed by remote host. (el host remoto cerró la conexión.)

Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5" para ver una lista completa de las propiedades de **cfgRacTune**.

La Tabla 11-16 muestra una lista de los parámetros definidos por el usuario.

Tabla 11-16. Propiedades de restricción de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presentan intentos fallidos consecutivos (**cfgRacTuneIpBlkFailCount**) provenientes de una misma dirección IP dentro de un periodo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecer una sesión que provengan de dicha dirección se rechazarán durante un periodo establecido (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El plazo en segundos dentro del que se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.
crgRacTuneIpBlkPenaltyTime	Define el periodo en segundos dentro del que se rechazan todos los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Activación del bloqueo de IP

El ejemplo a continuación evita que una dirección IP cliente establezca una sesión durante cinco minutos cuando el cliente a tenido cinco intentos fallidos de inicio de sesión dentro de un periodo de un minuto.

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente evita más de tres intentos fallidos dentro de un minuto y evita los intentos de inicio adicionales durante una hora.

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3


racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60


racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Establecimiento de la configuración de la seguridad de red por medio de la interfaz gráfica de usuario del DRAC 5

NOTA: Para realizar los pasos siguientes, debe tener permiso de **Configurar el DRAC 5**.

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Red**.
3. En la página **Configuración de red**, haga clic en **Configuración avanzada**.
4. En la página **Seguridad de la red**, configure los valores de los atributos y después haga clic en **Aplicar cambios**.

   La Tabla 11-17 describe los valores de la página **Seguridad de la red**.
5. Para continuar, haga clic en el botón adecuado de la página **Seguridad de la red**. Consulte la Tabla 11-18 para ver la descripción de los botones de la página **Seguridad de la red**.

Tabla 11-17. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de comprobación de rango de IP, lo que define el rango específico de direcciones IP que pueden tener acceso al DRAC 5.
Dirección del rango de IP	Determina la dirección de subred de IP aceptable.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en forma de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. Por ejemplo: **255.255.255.0**
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP.
Tiempo de penalización de bloqueo de IP	El periodo en segundos dentro del que se rechazan los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos.

Tabla 11-18. Botones de la página de seguridad de la red

Botón	Descripción
Imprimir	Imprime la página **Seguridad de la red**
Actualizar	Vuelve a cargar la página **Seguridad de la red**
Aplicar cambios	Guarda los cambios que se hagan en la página **Seguridad de la red**.
Volver a la página de configuración de la red>	Regresa a la página **Configuración de la red**.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de SM-CLP del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección contiene información sobre el 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 DRAC 5.

NOTA: Esta sección supone que el lector está familiarizado con la iniciativa SMASH (Arquitectura de administración de sistemas para hardware de servidor) y las especificaciones de SM-CLP de SMWG. Para obtener más información sobre estas especificaciones, visite el sitio web de DMTF (Grupo de trabajo de administración distribuida) en **www.dmtf.org**.

SM-CLP de DRAC 5 es un protocolo impulsado por el DMTF y el SMWG para ofrecer estándares para las implementaciones de CLI de administración de sistemas. El SM-CLP de SMWG es un subcomponente de los esfuerzos generales de SMASH que el DMTF supervisa.

Compatibilidad del DRAC 5 con SM-CLP

El DRAC 5 es el primer controlador de acceso remoto que es compatible con el protocolo de línea de comandos basado en el estándar SM-CLP. El SM-CLP se alberga en el firmware del controlador DRAC 5 y admite las interfaces Telnet, SSH y de conexión serie. La interfaz SM-CLP del DRAC 5 se basa en la versión 1.0 de la especificación SM-CLP que proviene de la organización DMTF.

Las secciones siguientes contienen una descripción general del componente SM-CLP que se ofrece desde el DRAC 5.

Funciones de SM-CLP

El SM-CLP promueve el concepto de verbos y destinos para brindar capacidades de administración de sistemas por medio de la CLI. El verbo indica la operación que se va a ejecutar y el destino determina la entidad (u objeto) que ejecuta la operación.

A continuación, se muestra un ejemplo de la sintaxis de la línea de comandos de SM-CLP.

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

Durante una sesión habitual de SM-CLP, el usuario puede realizar operaciones por medio de los verbos que aparecen en la Tabla 12-1 y en la Tabla 12-2.

Tabla 12-1. Verbos CLI admitidos para el sistema

Verbo	Definición
cd	Navega en el mapa por medio del shell.
delete	Elimina un objeto.
help	Muestra la ayuda de un destino específico.
reset	Restablece el destino.
show	Muestra las propiedades, verbos y destinos secundarios del destino.
start	Activa un destino.
stop	Desactiva un destino.
exit	Cierra la sesión de shell de SM-CLP.
version	Muestra los atributos de versión de un destino.

Tabla 12-2. Verbos CLI admitidos para operaciones de ventiladores, baterías, intrusión, rendimiento del hardware, suministros de energía, temperaturas y voltajes

Verbo	Definición
cd	Navega en el mapa por medio del shell.
help	Muestra la ayuda de un destino específico.
show	Muestra las propiedades, verbos y destinos secundarios del destino.
exit	Cierra la sesión de shell de SM-CLP.
version	Muestra los atributos de versión de un destino.

Uso de SM-CLP

1. Establezca una conexión SSH (o Telnet) con el DRAC 5 por medio de las credenciales correctas.
2. En la petición de comando, escriba `smclp`.

Se mostrará la indicación SMCLP (->).

Operaciones de administración y destinos de SM-CLP

Operaciones de administración

El SM-CLP de DRAC 5 permite que los usuarios administren lo siguiente:

- Administración de la alimentación de servidor: enciende, apaga o reinicia el sistema
- Administración de registro de sucesos del sistema: muestra o borra las anotaciones del registro de sucesos del sistema

Opciones

La Tabla 12-3 muestra una lista de las opciones admitidas de SM-CLP.

Tabla 12-3. Opciones admitidas de CM-CLP

Opción de SM-CLP	Descripción
-all	Indica al verbo que realice todas las funciones posibles.
-display	Muestra los datos definidos por el usuario.
-examine	Indica al procesador de comandos que valide la sintaxis del comando sin ejecutarlo.
-help	Muestra la ayuda del verbo de comando.
-version	Muestra la versión del verbo de comando.

Destinos

La Tabla 12-4 contiene una lista de los destinos que se proporcionan por medio de SM-CLP para sustentar estas operaciones.

Tabla 12-4. Destinos de SM-CLP

Destino	Definición
/sistema1	El destino de sistema administrado.
/sistema1/registros1	El destino de colecciones de registro
/sistema1/registros1/registro1	El destino del registro de sucesos de sistema en el sistema administrado.
/system1/logs1/log1/	Una anotación individual del registro de sucesos de sistema en el sistema administrado.

Anotación1	
/system1/pwrmgtsvc1	El servicio de administración de energía para el sistema.
/system1/pwrmgtsvc1/ pwrmgtcap1	Funciones del servicio de administración de energía para el sistema.
/system1/fan1	Destino de ventilador del sistema administrado.
/system1/fan1/ tachsensor1	Destino de sensor individual correspondiente al ventilador de destino del sistema administrado.
/system1/batteries1	Destino de batería del sistema administrado.
/system1/batteries1/ sensor1	Destino de sensor individual correspondiente a la batería de destino del sistema administrado.
/system1/intrusion1	Destino de intrusión del chasis del sistema administrado.
/system1/intrusion1/ sensor1	Destino de sensor individual correspondiente al destino de intrusión del chasis del sistema administrado.
/system1/hardwareperformance1	Destino de rendimiento del hardware del sistema administrado.
/system1/hardwareperformance1/sensor1	Destino de sensor individual correspondiente al destino de rendimiento del hardware del sistema administrado.
/system1/powersupplies1	Destino de suministro de energía del sistema administrado.
/system1/powersupplies1/sensor1	Destino de sensor individual correspondiente al destino de suministro de energía del sistema administrado.
/system1/temperatures1	Destino de temperatura del sistema administrado.
/system1/temperatures1/tempsensor1	Destino de sensor individual correspondiente al destino de temperatura del sistema administrado.
/system1/voltages1	Destino de voltaje del sistema administrado.
/system1/voltages1/voltsensor1	Destino de sensor individual correspondiente al destino de voltaje del sistema administrado.
/system1/chassis1	Destino de chasis individual del sistema.

Formato de salida de SM-CLP

El DRAC 5 actualmente es compatible con los mensajes de salida de texto que se describen en las especificaciones de SM-CLP.

Ejemplos de SM-CLP del DRAC 5

Los apartados siguientes contienen escenarios de ejemplo sobre cómo usar el SM-CLP para realizar las siguientes operaciones:

- Administración de la alimentación del servidor
- Administración del registro de sucesos del sistema
- Navegación del mapa de destino
- Mostrar las propiedades del sistema

Administración de la alimentación del servidor

La Tabla 12-5 contiene ejemplos de cómo usar el SM-CLP para realizar operaciones de administración de la alimentación del servidor en un sistema administrado.

Tabla 12-5. Operaciones de administración de la alimentación del servidor

Operación	Sintaxis
Iniciar sesión en el RAC por medio de la interfaz Telnet o SSH	>ssh 192.168.0.120 >login: root >password:
Iniciar el shell de administración de SM-CLP	- >smclp DRAC5 SM-CLP System Management Shell, version 1.0 Copyright (c) 2004-2008 Dell, Inc. All Rights Reserved ->
Apagar el servidor	

	- ->stop /system1 system1 has been stopped successfully
Encender el servidor a partir de un estado apagado	- ->start /system1 system1 has been started successfully
Reiniciar el servidor	->reset /system1 system1 has been reset successfully

Administración del registro de sucesos del sistema

La Tabla 12-6 contiene ejemplos de cómo usar el SM-CLP para ejecutar operaciones relacionadas con el registro de sucesos del sistema en el sistema administrado.

Tabla 12-6. Operaciones de administración del registro de sucesos del sistema

Operación	Sintaxis
Ver el registro de sucesos del sistema	->show /system1/logs1/log1 /system1/logs1/log1 Targets: Record1 Record2 Record3 Record4 Record5 Properties: InstanceID = IPMI:BMC1 SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL Description = IPMI SEL ElementName = IPMI SEL Commands: cd show help exit version
Ver la anotación del registro de sucesos del sistema	->show /system1/logs1/log1/record4 /system1/logs1/log1/record4 Properties: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512.000000- 000 Description = FAN 7 RPM: fan sensor, detected a failure ElementName = IPMI SEL Record Commands: cd show help exit version
Borrar el registro de sucesos del sistema	->delete /system1/logs1/log1/record* All records deleted successfully

Administración de las baterías

La Tabla 12-7 ofrece ejemplos del uso de SM-CLP para ejecutar operaciones relacionadas con las baterías.

Tabla 12-7. Operaciones de administración de las baterías

Operación	Sintaxis
Visualización del estado de las baterías	->show system1/batteries1/sensor1 /system1/batteries1/sensor1: Properties: SystemCreationClassName = CIM_ComputerSystem SystemName = F196P1S CreationClassName = CIM_Sensor DeviceID = BATTERY 1 SensorType = 1 PossibleStates = {"Good" "Bad" "Unknown"} CurrentState = good ElementName = System Board CMOS Battery OtherSensorTypeDescription = CMOS battery sensor. EnabledState = 1 Verbs: cd exit help show version

Navegación del mapa de destino

La Tabla 12-8 muestra ejemplos de cómo usar el verbo cd para navegar el mapa. En todos los ejemplos, se supone que el destino inicial predeterminado es /.

Tabla 12-8. Operaciones de navegación del mapa de destino

Operación	Sintaxis
Navegar hacia el sistema destino y reiniciar	->cd system1 ->reset **NOTA:** El destino predeterminado actual es /.
Navegar hacia el registro de sucesos del sistema de destino y mostrar las anotaciones del registro	->cd system1 ->cd logs1/log1 ->show
	->cd system1/logs1/log1 ->show
Mostrar el destino actual	->cd .
Subir un nivel	->cd ..
Salir del shell	->exit

Propiedades del sistema

La Tabla 12-9 muestra una lista de las propiedades del sistema que se muestran cuando el usuario escribe lo siguiente:

```
show /system1
```

Estas propiedades se derivan del perfil del sistema base proporcionado por el cuerpo de estándares u se basa en la clase **CIM_ComputerSystem** según se define en el esquema CIM.

Para obtener información adicional, consulte las definiciones del esquema CIM de DMTF.

Tabla 12-9. Propiedades del sistema

Objeto	Propiedad	Descripción
CIM_ComputerSystem	Nombre	Identificador único de un sistema que existe en el entorno empresarial. MaxLen = 256
	ElementName	Nombre nemotécnico del sistema. MaxLen = 64
	NameFormat	Identifica el método mediante el cual se genera el nombre. Valores: Other, IP, Dial, HID, NWA, HWA, X25, ISDN, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	Dedicado	Enumeración que indica si el sistema es un sistema para fines específicos o un sistema para fines generales. Valores: 0=No dedicado 1=Desconocido 2=Otro 3=Almacenamiento 4=Ruteador

	5=Conmutador 6=Conmutador de capa 3 7=Conmutador de oficina central 8=Concentrador 9=Servidor de acceso 10=Servidor de seguridad 11=Impresión 12=E/S 13=Caché de web 14=Administración 15=Servidor de bloqueo
	16=Servidor de archivos 17=Dispositivo de usuario móvil, 18=Repetidor 19=Puente/ampliador 20=Puerta de enlace 21=Virtualizador de almacenamiento 22=Biblioteca de medios 23=Nodo ampliador 24=Cabezal de NAS 25=NAS autocontenido 26=UPS 27=Telefonía IP 28=Controlador de administración 29=Administrador de chasis
ResetCapability	Define los métodos de restablecimiento que están disponibles en el sistema Valores: 1=Otro 2=Desconocido 3=Desactivado 4=Activado 5=No implementado
CreationClassName	La súper clase a partir de la cual se deriva esta instancia.
EnabledState	Indica los estados activado o desactivado del sistema. Valores: 0=Desconocido 1=Otro 2=Activado 3=Desactivado 4=Apagándose 5=No se aplica 6=Activado pero fuera de línea 7=En prueba

	8=Diferido 9=Temporalmente inactivo 10=Iniciándose
EnabledDefault	Indica la configuración de inicio predeterminada del estado activado del sistema. De manera predeterminada, el sistema esta "Activado" (valor=2). Valores: 2=Activado 3=Desactivado 4=No se aplica 5=Activado pero fuera de línea 6=Sin valor predeterminado
RequestedState	Indica el último estado solicitado o deseado del sistema. Valores: 2=Activado 3=Desactivado 4=Apagar 5=Sin cambios 6=Fuera de línea 7=Probar 8=Diferido 9=Temporalmente inactivo 10=Reiniciar 11=Restablecer 12=No se aplica
HealthState	Indica la condición actual del sistema. Valores: 0=Desconocido 5=En buen estado 10=Degradado/advertencia 15=Falla menor 20=Falla mayor 30=Falla crítica 35=Error no recuperable
OperationalStatus	Indica el estado actual del sistema. Valores: 0=Desconocido 1=Otro 2=En buen estado 3=Degradado 4=Bajo presión 5=Falla predecible 6=Error 7=Error no recuperable 8=Iniciándose 9=Deteniéndose

		10=Detenido 11=En servicio 12=Sin contacto 13=Se perdió la comunicación 14=Anulado 15=Dormido 16=Entidad admitida presenta error 17=Completado 18=Modo de alimentación
	Descripción	Texto con una descripción del sistema.

Nombres de propiedades para sensores de ventiladores, temperatura, voltaje numérico, consumo de energía y amperaje

Nombres de propiedades admitidas para sensores de ventiladores, temperatura, voltaje numérico, consumo de energía y amperaje

Tabla 12-10. Sensores

Objeto	Propiedad	Descripción
CIM_NumericSensor	SystemCreationClassName	Nombre de la clase de creación del sistema: CIM_ComputerSystem)
	SystemName	La etiqueta de servicio del sistema, esto es, el identificador exclusivo de un sistema que existe en el entorno empresarial
	CreationClassName	Nombre de la clase de creación: CIM_NumericSensor
	DeviceID	Identificador exclusivo del sensor en el sistema fan1...n (para tachsensor) temp 1...n (para tempsensor) numeric voltage 1...n) para numericsensor (voltaje) (sólo sistemas PMBus)) power consumption 1...n (para consumo de energía (sólo sistemas PMBus)) amperage 1...n (para amperaje (sólo sistemas PMBus))
	BaseUnits	Unidades de medida del sensor RPM= tachómetro (para tachsensor) C= temperatura (para tempsensor) V= voltaje (para numericsensor) Watts= consumo de energía (para powerconsumption) Amp= amperaje (para amperaje)
	CurrentReading	Lectura actual del sensor.
	LowerThresholdNonCritical	Valor no crítico de umbral mínimo
	UpperThresholdNonCritical	Valor no crítico de umbral máximo
	LowerThresholdCritical (umbral inferior crítico)	Valor crítico de umbral mínimo
	UpperThresholdCritical (umbral superior crítico)	Valor crítico de umbral máximo
	SupportedThreshold	Umbral admitido para el sensor. { "LowerThresholdCritical" } (para tachsensor) { "LowerThresholdNonCritical", "UpperThresholdNonCritical", "UpperThresholdCritical", "LowerThresholdCritical" } (para tempsensor) {} (para voltsensor (sensor numérico)) {"UpperThresholdNonCritical", "UpperThresholdCritical"} (para powerconsumption {} para amperaje)
	SettableThreshold	Niveles de umbral que pueden definirse para un sensor. { } (el sensor no admite la definición de valores de umbral)
	SensorTypes	Tipos de sensor: 5= tachómetro (para tachsensor) 2= temperatura (para temperatura) 3= voltaje (para voltaje) 1= consumo de energía (para powerconsumption) 1= amperaje (para amperaje)
	PossibleStates	Posibles estados del sensor.

		{ "unknown", "warning", "failed", "non-recoverable" }
	CurrentState	El estado actual indicado por un sensor
	ElementName	Nombre del sensor
	OtherSensorTypeDescription	Si la propiedad sensortype contiene el valor "1" (otros), brindará información adicional acerca del sensor. "Power consumption sensor." para powerconsumption "Amperage sensor." para amperaje
	EnabledState	Indica si el sensor está activado o desactivado. 1= activado

Nombres de propiedades para sensores de suministro de energía

Tabla 12-11. Nombres de propiedades admitidas para sensores de suministro de energía

Objeto	Propiedad	Descripción
CIM_NumericSensor	SystemCreationClassName	Nombre de la clase de creación del sistema: CIM_ComputerSystem)
	SystemName	La etiqueta de servicio del sistema, esto es, el identificador exclusivo de un sistema que existe en el entorno empresarial
	CreationClassName	Nombre de la clase de creación: CIM_PowerSupply
	DeviceID	Identificador exclusivo del sensor en el sistema. pwrsupply 1...n
	TotalOutputPower	Salida total de energía tal como se muestra en la interfaz del usuario del DRAC
	ElementName	Nombre de ese sensor en particular.
	OperationalStatus	Estado operativo actual de la unidad de suministro de energía.
	HealthState	Estado general de la unidad de suministro de energía.
	EnabledState	Indica si el sensor está activado o desactivado 1= activado

Nombres de propiedades para sensores de rendimiento de intrusión, baterías, voltaje y hardware

Tabla 12-12. Nombres de propiedades admitidas para sensores de rendimiento de intrusión, baterías, voltaje y hardware

Objeto	Propiedad	Descripción
CIM_NumericSensor	SystemCreationClassName	Nombre de la clase de creación del sistema: CIM_ComputerSystem)
	SystemName	La etiqueta de servicio del sistema, esto es, el identificador exclusivo de un sistema que existe en el entorno empresarial
	CreationClassName	Nombre de la clase de creación: CIM_Sensor
	DeviceID	Identificador exclusivo del sensor en el sistema Intrusion1...n (para sensor de intrusión) Battery1...n (para sensor de batería) Voltage1...n (para sensor de voltaje) Hardware performance sensor1...n (para sensor de rendimiento de hardware)
	SensorType	1=Otro 3= voltaje (para sensor de voltaje)
	PossibleStates	Posibles estados del sensor { "no intrusion", "chassis intrusion," "drive bay intrusion," "I/O card area intrusion," "processor area intrusion," "LAN disconnect," "unauthorized dock," "FAN area intrusion" } (para el sensor de intrusión) { "absent," "low," "failed," "good" } (para el sensor de batería) { "good," "bad," "unknown" } (para el sensor de voltaje) { "Normal," "Others," "Thermal Protection," "Cooling Capacity changed," "Power Capacity changed," "User Configuration" } (para el sensor de rendimiento de hardware)
	CurrentState	Estado actual indicado por el sensor.
	ElementName	Nombre del sensor
	OtherSensorTypeDescription	Si la propiedad sensortype contiene el valor "1" (otros), brindará información adicional acerca del

		sensor. "Chassis intrusion sensor" (para el sensor de intrusión) "CMOS battery sensor" (para el sensor de batería) "Hardware performance sensor" (para rendimiento de hardware)
	EnabledState	Indica si el sensor está activado o desactivado 1= activado (para todos los sensores)

Nombres de propiedades para sensores de redundancia de ventiladores y suministro de energía

Tabla 12-13. Nombres de propiedades admitidas para sensores de redundancia de ventiladores y suministro de energía

Objeto	Propiedad	Descripción
CIM_RedundancySet	InstanceID	Número de la instancia
	RedundancyStatus	Estado de redundancia.
	TypeOfSet	3= carga equilibrada (para la redundancia del ventilador) 4= moderada (para la redundancia de suministro de energía)
	MinNumberNeeded	0=Desconocido
	ElementName	Nombre del sensor

Nombres de propiedades para sensores de chasis

Tabla 12-14. Nombres de propiedades admitidas para sensores de chasis

Objeto	Propiedad	Descripción
CIM_Chassis	CreationClassName	Nombre de la clase de creación: CIM_Chassis
	PackageType	Tipo de paquete 3= chasis
	ChassisPackageType	Tipo de paquete de chasis 17= chasis del sistema principal
	Fabricante	Fabricante "Dell"
	Model	Nombre de modelo del sistema.
	ElementName	Nombre de elemento

Nombres de propiedades para servicio de administración de energía

Tabla 12-15. Nombres de propiedades admitidas para servicio de administración de energía

Objeto	Propiedad	Descripción
CIM_PowerManagementService	CreationClassName	Nombre de la clase de creación: CIM_PowerManagementService
	Nombre	Servicio de energía IPMI
	ElementName	Servicio de administración de energía de Dell Server
	powerstate	Estado de energía actual del sistema 2= encendido 6= apagado Pueden definirse los siguientes valores: 2= encendido

		6= apagado 5= restablecimiento de energía 9= ciclo de encendido del sistema

El verbo set le permite definir el estado de energía del sistema. Por ejemplo, para encender el sistema si está apagado:

```
set powerstate=2
```

Nombres de propiedades para capacidad de energía

Tabla 12-16. Nombres de propiedades admitidas para capacidad de energía

Objeto	Propiedad	Descripción
CIM_PowerManagementCapabilities	InstanceID	Identificador de instancia exclusivo para las funciones de energía
	PowerChangeCapabilities	3= estado de energía definible
	ElementName	Servicio de administración de energía de Dell Server
	PowerStatesSupported	2= encendido 6= apagado 5= restablecimiento de energía 9= ciclo de encendido del sistema

---

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alertas

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

En esta sección se explica cómo supervisar el DRAC 5 y se describen los procedimientos para configurar el sistema y el DRAC 5 para recibir alertas.

Configuración del sistema administrado para capturar la pantalla del último bloqueo

Antes de que el DRAC 5 pueda capturar la pantalla de último bloqueo, se debe configurar el sistema administrado con los siguientes prerrequisitos.

1. Instale el software de sistema administrado. Para obtener más información sobre la instalación del software Managed System, consulte la *Guía del usuario de Server Administrator*.
2. Ejecute un sistema operativo admitido Microsoft® Windows® con la función de "reinicio automático" de Windows deseleccionada en la **Configuración de inicio y recuperación de Windows**.
3. Active la pantalla de último bloqueo (desactivada de manera predeterminada).

   Para activarla por medio de RACADM local, abra una petición de comandos y escriba los comandos siguientes:

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

4. Active el temporizador de recuperación automática y defina la acción Recuperación automática como **Restablecer**, **Apagar** o **Ciclo de encendido**. Para configurar el temporizador de Recuperación automática, debe usar Server Administrator o IT Assistant.

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

   La pantalla de último bloqueo no está disponible cuando la acción Recuperación automática se establece como **Apagar** o **Ciclo de encendido** si el sistema administrado está apagado.

Desactivación de la opción de reinicio automático de Windows

Para garantizar que la función de pantalla de último bloqueo de la interfaz basada en web del DRAC 5 funcione correctamente, desactive la opción **Reinicio automático** en los sistemas administrados que ejecuten los sistemas operativos Microsoft Windows Server 2003 y Windows 2000 Server.

Desactivación de la opción de reinicio automático en Windows Server 2003

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

Desactivación de la opción de reinicio automático en Windows 2000 Server

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.
2. Haga clic en la ficha **Opciones avanzadas**.
3. Haga clic en el botón **Inicio y recuperación...**.

4. Deseleccione la casilla **Reiniciar automáticamente**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma tiene un mecanismo para configurar el dispositivo de acceso remoto a fin de realizar las acciones seleccionadas ante ciertos mensajes de sucesos. Estas acciones incluyen reiniciar, ciclo de encendido, apagar y enviar una alerta (Captura de sucesos de plataforma [PET] y/o por correo electrónico).

Los sucesos de plataforma que se pueden filtrar incluyen los siguientes:

- Falla de sonda del ventilador
- Advertencia de sonda de baterías
- Falla de sonda de baterías
- Falla discreta de sonda de voltaje
- Advertencia de sonda de temperatura
- Falla de sonda de temperatura
- Intromisión al chasis detectada
- Redundancia degradada
- Redundancia perdida
- Advertencia del procesador
- Falla del procesador
- Procesador ausente
- Advertencia de PS/VRM/D2D
- Falla de PS/VRM/D2D
- Suministro de energía ausente
- Falla del registro de hardware
- Recuperación automática de sistema

Cuando se presenta un suceso de plataforma (por ejemplo, una falla de la sonda de ventilador), el suceso se genera y se registra en el registro de sucesos del sistema. Si este suceso coincide con un filtro de sucesos de plataforma (PEF) en la lista de filtros de sucesos de plataforma de la interfaz basada en web y usted ha configurado este filtro para que genere una alerta (PET o por correo electrónico), se enviará una alerta de PET o por correo electrónico a un conjunto de uno o más destinos configurados.

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

Configuración de los filtros de sucesos de plataforma (PEF)

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

Configuración de PEF por medio de la interfaz de usuario basada en web

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte "Acceso a la interfaz basada en web".
2. Haga clic en la ficha **Administración de alertas** y después haga clic en **Sucesos de plataforma**.
3. Active las alertas globales.
   a. Haga clic en **Administración de alertas** y seleccione **Sucesos de plataforma**.
   b. Seleccione la casilla **Activar alerta de filtro de sucesos de plataforma**.
4. En **Configuración de filtros de sucesos de plataforma**, seleccione la casilla **Activar filtros de alerta de sucesos de plataforma** y después haga clic en **Aplicar cambios**.
5. En la **Lista de los filtros de sucesos de plataforma**, haga doble clic en el filtro que desea configurar.
6. En la página **Definir sucesos de plataforma**, elija las selecciones adecuadas y después haga clic en **Aplicar cambios**.

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

Configuración de PEF por medio de la CLI de RACADM

1. Active el PEF.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
   ```

   donde `1` y `1` son el índice de PEF y la selección de activación/desactivación, respectivamente.

   El índice de PEF puede ser un valor de 1 a 17. La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar un PEF con índice 5, escriba el comando siguiente:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
   ```

2. Configure las acciones de PEF.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <acción>
   ```

   donde los bits de los valores *<acción>* son los siguientes:

   - Un bit 0 de valor de *<acción>* de 1= activar la acción de alerta, 0 = desactivar la alerta
   - Un bit 1 de valor de *<acción>* de 1 = apagar; 0 = no apagar
   - Un bit 2 de valor de *<acción>* de 1 = reiniciar; 0 = no reiniciar
   - Un bit 3 de valor de *<acción>* de 1 = realizar ciclo de encendido; 0 = no realizar ciclo de encendido

   Por ejemplo, para hacer que el PEF reinicie el sistema, escriba el siguiente comando:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
   ```

   donde `1` es el índice de PEF y 2 es la acción del PEF de reiniciar.

Configuración de la PET

Configuración de la PET por medio de la interfaz de usuario basada en web

1. Inicie sesión en el sistema remoto con un explorador de web compatible. Consulte "Acceso a la interfaz basada en web".
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de PEF por medio de la interfaz de usuario basada en web".
3. Configure la política de PET.
   a. En la ficha **Administración de alertas**, haga clic en **Configuración de capturas**.
   b. En **Valores de configuración del destino**, configure el campo **Cadena de comunidad** con la información correspondiente y después haga clic en **Aplicar cambios**.
4. Configure la dirección IP de destino de la PET

a. En la columna **Número de destino** , haga clic en un número de destino.

b. Compruebe que la casilla **Activar destino** esté seleccionada.

c. En el campo **Dirección IP de destino**, escriba una dirección IP válida de destino de la PET.

d. Haga clic en **Aplicar cambios**.

e. Haga clic en **Enviar captura de prueba** para probar la alerta configurada (si lo desea).

NOTA: La cuenta de usuario debe tener permiso de **Probar alertas** para poder realizar este procedimiento. Consulte el apartado Tabla 5-4.

f. Repita del paso a al paso e para los números de destino restantes.

Configuración de PET por medio de la CLI de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active la PET.

   En la petición de comandos, escriba los comandos siguientes y presione <Entrar> después de cada comando:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
   ```

   donde `1` y `1` son el índice de destino de PET y la selección de activación/desactivación, respectivamente.

   El índice de destino de PET puede ser un valor de 1 a 4. La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar una PET con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
   ```

3. Configure la política de PET.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <dirección_IP>
   ```

   donde `1` es el índice de destino de la PET y *<dirección_IP>* es la dirección IP de destino del sistema que recibe las alertas de sucesos de plataforma.

4. Configure la cadena de nombre de comunidad.

   En el indicador de comandos, escriba:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Nombre>
   ```

Configuración de alertas por correo electrónico

Configuración de alertas por correo electrónico por medio de la interfaz de usuario basada en web

1. Inicie sesión en el sistema remoto con un explorador de web compatible. Consulte "Acceso a la interfaz basada en web".
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de PEF por medio de la interfaz de usuario basada en web".
3. Configure los valores de la alerta de correo electrónico.
   a. En la ficha **Administración de alertas**, haga clic en **Configuración de alertas por correo electrónico**.
   b. En **Configuración de la dirección del servidor SMTP (correo electrónico)**, configure el campo **Dirección del servidor SMTP (correo electrónico)** con la información correspondiente y después haga clic en **Aplicar cambios**.
4. Configure el destino de la alerta por correo electrónico.
   a. En la columna **Número de alerta por correo electrónico**, haga clic en un número de alerta por correo electrónico.
   b. Compruebe que la casilla **Activar la alerta por correo electrónico** esté seleccionada.
   c. En el campo **Dirección de correo electrónico de destino**, escriba una dirección válida de correo electrónico.
   d. En el campo **Descripción del correo electrónico**, introduzca una descripción (si es necesaria).
   e. Haga clic en **Aplicar cambios**.
   f. Haga clic en **Enviar correo electrónico de prueba** para probar la alerta por correo electrónico que configuró (si así lo desea).

   NOTA: La cuenta de usuario debe tener permiso de **Probar alertas** para poder realizar este procedimiento. Consulte el apartado Tabla 5-4.

   g. Repita del paso a al paso e para los valores de las alertas por correo electrónico restantes.
5. Active las alertas globales.
   a. Haga clic en **Administración de alertas** y seleccione **Sucesos de plataforma**.
   b. Seleccione la casilla **Activar alerta de filtro de sucesos de plataforma**.

Configuración de alertas de correo electrónico por medio de la CLI de RACADM

1. Active las alertas globales.

   Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico.

   En la petición de comandos, escriba los comandos siguientes y presione <Entrar> después de cada comando:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
   ```

   `donde 1 y 1` son el índice de destino de correo electrónico y la selección de activación/desactivación, respectivamente.

   El índice de destino de correo electrónico puede ser un valor de 1 a 4. La selección de activación o desactivación puede ser 1 (activado) o 2 (desactivado).

   Por ejemplo, para activar un correo electrónico con índice 4, escriba el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configure los valores del correo electrónico.

   En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

   `racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>`

donde 1 es el índice de destino de correo electrónico y *<dirección_de_correo_electrónico>* es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

Para configurar un mensaje personalizado, en la petición de comandos escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <mensaje_personalizado>
```

donde 1 es el índice de destino de correo electrónico y *<mensaje_personalizado>* es el mensaje personalizado.

Comprobación de las alertas por correo electrónico

La función de alertas por correo electrónico del RAC permite que los usuarios reciban alertas por correo electrónico cuando se presenta un suceso crítico en el sistema administrado. El ejemplo a continuación muestra cómo probar la función de envío de alertas por correo electrónico para garantizar que el RAC pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Compruebe que los valores de **SMTP** y **Alerta por correo electrónico** estén configurados antes de probar la función de envío de alertas por correo electrónico. Consulte "Configuración de alertas por correo electrónico" para obtener más información.

Comprobación de la función de alertas de captura SNMP del RAC

La función de alertas de captura SNMP del RAC permite que las configuraciones del detector de capturas SNMP para recibir capturas para sucesos de sistema que se presenten en el sistema administrado.

El siguiente ejemplo muestra la manera en la que un usuario puede probar la función de alertas de capturas SNMP del RAC.

```
racadm testtrap -i 2
```

Antes de probar la función de alertas de capturas SNMP del RAC, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Consulte las descripciones de los comandos "**testtrap**" y "**testemail**" para configurar estos valores.

Preguntas más frecuentes

¿Por qué aparece el siguiente mensaje?

Remote Access: SNMP Authentication Failure (Acceso remoto: error de autenticación de SNMP)

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad Get y Set del dispositivo. En IT Assistant, usted tiene el nombre de comunidad Get = public y el nombre de comunidad Get = private. De manera predeterminada, el nombre de comunidad del agente de DRAC 5 es "public". Cuando IT Assistant envía una solicitud, el agente de DRAC 5 genera el error de autenticación de SNMP porque sólo aceptará solicitudes de comunidad = public.

Usted puede cambiar el nombre de comunidad de DRAC 5 por medio de RACADM.

Para ver el nombre de comunidad de DRAC 5, utilice el siguiente comando:

```
racadm getconfig -g cfgOobSnmp
```

Para establecer el nombre de comunidad de DRAC 5, utilice el siguiente comando:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nombre de comunidad>
```

Para evitar que se generen capturas de autenticación de SNMP, se deben introducir nombres de comunidad que el agente acepte. Como el DRAC 5 sólo permite un nombre de comunidad, se debe usar el mismo nombre de comunidad get y set para la configuración de descubrimiento de IT Assistant.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la Interfaz de administración de plataforma inteligente (IPMI)

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Configuración de IPMI

Esta sección contiene información sobre cómo configurar y usar la interfaz IPMI del DRAC 5. La interfaz incluye lo siguiente:

- IPMI mediante la LAN
- IPMI en la conexión serie
- Comunicación en serie en la LAN

El DRAC 5 es totalmente compatible con IPMI 2.0. Puede configurar la IPMI del DRAC por medio de:

- su explorador
- una utilidad de código abierto, como *ipmitool*
- el shell de IPMI de Dell OpenManage, **ipmish**
- RACADM.

Para obtener más información sobre cómo usar el shell de IPMI, ipmish, consulte la *Guía del usuario del BMC de Dell OpenManage*™ que se encuentra en el sitio web de asistencia de Dell en **support.dell.com**.

Para obtener más información sobre cómo usar RACADM, consulte "Uso de RACADM de manera remota".

Configuración de IPMI por medio de la interfaz basada en web

1. Inicie sesión en el sistema remoto con un explorador de web compatible. Consulte "Acceso a la interfaz basada en web".
2. Configure la IPMI en la LAN.
   a. En el árbol **Sistema**, haga clic en **Acceso remoto**.
   b. Haga clic en la ficha **Configuración** y haga clic en **Red**.
   c. En la página **Configuración de red** en **Configuración de LAN de IPMI**, seleccione **Activar IPMI en la LAN** y haga clic en **Aplicar cambios**.
   d. Actualice los privilegios del canal de LAN de IPMI, si es necesario.

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

   En **Configuración de LAN de IPMI**, haga clic en el menú desplegable **Límite de nivel de privilegios del canal**, seleccione **Administrador**, **Operador** o **Usuario** y haga clic en **Aplicar cambios**.
   e. Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

   NOTA: La IPMI del DRAC 5 admite el protocolo RMCP+.

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

   NOTA: La clave de cifrado debe consistir en un número par de caracteres hexadecimales con un máximo de 40 caracteres.
3. Configure la comunicación en serie en la LAN (SOL) de IPMI.

a. En el árbol **Sistema**, haga clic en **Acceso remoto**.

b. En la ficha **Configuración**, haga clic en **Comunicación en serie en la LAN**.

c. En la página **Configuración de la comunicación en serie en la LAN**, seleccione **Activar comunicación en serie en la LAN**.

d. Actualice la velocidad en baudios de la SOL de IPMI.

NOTA: Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

e. Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

f. Actualice el **Privilegio mínimo requerido.** Esta propiedad define el privilegio mínimo de usuario que se requiere para usar la función **Comunicación en serie en la LAN**.

Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Usuario**, **Operador** o **Administrador**.

g. Haga clic en **Aplicar cambios**.

4. Configure la conexión serie de IPMI.

a. En la ficha **Configuración**, haga clic en **Serie**.

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

En **Conexión serie de IPMI**, haga clic en el menú desplegable **Valor del modo de conexión** y seleccione el modo adecuado.

c. Establezca la velocidad en baudios de la conexión serie de IPMI.

Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.

d. Establezca el límite del nivel de privilegios de canal.

Haga clic en el menú desplegable **Límite del nivel de privilegios de canal**, seleccione **Administrador**, **Operador** o **Usuario**.

e. Haga clic en **Aplicar cambios**.

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

- Reinicie el sistema.
- Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
- Diríjase a **Comunicación serie**.
- En el menú **Conexión serie**, compruebe que **Conector serie externo** esté definido como **Dispositivo de acceso remoto**.
- Guarde los cambios y salga del programa de configuración del BIOS.
- Reinicie el sistema.

Si la conexión serie de IPMI está en modo de terminal, puede configurar los siguientes valores adicionales:

- Control de eliminación
- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Configuración de IPMI por medio de la CLI de RACADM

1. Inicie sesión en el sistema remoto por medio de cualquiera de las interfaces de RACADM. Consulte "Uso de RACADM de manera remota".
2. Configure la IPMI en la LAN.

Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

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

a. Actualice los privilegios de canal de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>
```

donde <*nivel*> es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para definir el privilegio de canal de LAN de IPMI en 2 (usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

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

NOTA: La IPMI del DRAC 5 admite el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>
```

donde <*clave*> es una clave de cifrado de 20 caracteres en formato hexadecimal válido.

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

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Actualice el nivel de privilegios mínimo de SOL de IPMI.

El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación IPMI 2.0.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>
```

donde <*nivel*> es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para configurar los privilegios de IPMI como 2 (usuario), escriba el siguiente comando:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. Actualice la velocidad en baudios de la SOL de IPMI.

NOTA: Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_en_baudios>
```

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo,

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Active la SOL.

NOTA: Cada usuario individual puede activar o desactivar la SOL.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

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

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

4. Configure la conexión serie de IPMI.

a. Cambie el modo de conexión serie de IPMI al valor adecuado.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

b. Establezca la velocidad en baudios de la conexión serie de IPMI.

Abra una petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <velocidad_en_baudios>
```

donde <*velocidad_en_baudios*> es 9600, 19200, 57600 ó 115200 bps.

Por ejemplo,

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. Active el control de flujo del hardware de la conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

d. Establezca el nivel mínimo de privilegios de canal de conexión serie de IPMI.

En la petición de comandos, escriba el comando siguiente y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>
```

donde <*nivel*> es uno de los siguientes:

- 2 (Usuario)
- 3 (Operador)
- 4 (Administrador)

Por ejemplo, para definir los privilegios de canal de conexión serie de IPMI en 2 (usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. Compruebe que multiplexor serie esté configurado correctamente en el programa de configuración del BIOS.

- Reinicie el sistema.
- Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
- Diríjase a **Comunicación serie**.
- En el menú **Conexión serie**, compruebe que **Conector serie externo** esté definido como **Dispositivo de acceso remoto**.
- Guarde los cambios y salga del programa de configuración del BIOS.
- Reinicie el sistema.

La configuración de IPMI ha terminado.

Si la conexión serie de IPMI está en modo de terminal, usted puede configurar los siguientes valores adicionales por medio de los comandos **racadm config cfgIpmiSerial**:

- Control de eliminación
- Control de eco
- Edición de línea
- Secuencias de nueva línea
- Entrada de secuencias de nueva línea

Para obtener más información sobre estas propiedades, consulte la especificación IPMI 2.0.

Uso de la interfaz serie de acceso remoto de IPMI

Los siguientes modos están disponibles en la interfaz serie de IPMI:

- **Modo de terminal de IPMI**: admite comandos ASCII provenientes de una terminal serie. El conjunto de comandos tiene un número limitado de comandos (que incluye el control de potencia) y admite comandos de IPMI sin procesar que se introduzcan como caracteres ASCII hexadecimales.
- **Modo básico de IPMI**: admite una interfaz binaria para acceso a programa, como el shell de IPMI (IPMISH) que se incluye con la Utilidad de administración de la placa base (BMU).

Para configurar el modo de IPMI por medio de RACADM:

1. Desactive la interfaz serie del RAC.

   En el indicador de comandos, escriba:

   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```

2. Active el modo IPMI adecuado.

   Por ejemplo, en la petición de comandos, escriba:

   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 ó 1>
   ```

Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5" para obtener información.

Configuración de la comunicación en serie en la LAN

NOTA: Para completar la información de la Conexión en serie en la LAN, consulte la *Guía del usuario del controlador de administración de la placa base de Dell OpenManage*.

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Comunicación serie en la LAN**.
3. Configure los valores de la comunicación en serie en la LAN.

   La Tabla 14-1 contiene información sobre los valores de la página **Configuración de la comunicación en serie en la LAN**.

4. Haga clic en **Aplicar cambios**.
5. Defina la configuración avanzada, si es necesario. De lo contrario, haga clic en el botón correspondiente de la página **Configuración de la comunicación en serie en la LAN** para continuar (consulte la Tabla 14-2).

   Para definir la configuración avanzada:

   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 el apartado Tabla 14-3.

   c. Haga clic en **Aplicar cambios**.

   d. Haga clic en el botón correspondiente de la página **Configuración avanzada de la comunicación en serie en la LAN** para continuar. Consulte la Tabla 14-4 o la descripción de los botones de la página **Configuración avanzada de la comunicación en serie en la LAN**.

Tabla 14-1. Valores de la página de configuración de la comunicación en serie en la LAN

Valor	Descripción
Activar comunicación en serie en la LAN.	Activa la comunicación en serie en la LAN. Seleccionada=activado; deseleccionada=desactivado.
Velocidad en baudios	La velocidad de los datos de IPMI. Seleccione **9600 bps**, **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.
Límite del nivel de privilegios del canal	Establezca el privilegio mínimo de usuario de la comunicación en serie en la LAN de IPMI: **Administrador**, **Operador** o **Usuario**.

Tabla 14-2. Botones de la página de configuración de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime la página **Configuración de la comunicación en serie en la LAN**.

Actualizar	Actualiza 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 cambios	Aplica los valores de la página **Configuración de la comunicación en serie en la LAN**.

Tabla 14-3. 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 BMC esperará antes de transmitir un paquete parcial de datos de caracteres de SOL. Incrementos de 5 ms basados en 1.
Umbral de envío de caracteres	El BMC enviará un paquete de datos de caracteres de SOL que contiene los caracteres tan pronto como este número de caracteres (o un número mayor) haya sido aceptado. Unidades basadas en 1.

Tabla 14-4. Botones de la página de configuración avanzada de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime la página **Configuración avanzada de la comunicación en serie en la LAN**.
Actualizar	Actualiza 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 a la página **Configuración de la comunicación en serie en la LAN**.
Aplicar cambios	Aplica los valores de la página **Configuración avanzada de la comunicación en serie en la LAN**.

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del sistema administrado

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección explica cómo realizar las siguientes tareas relacionadas con la recuperación y solución de problemas de un sistema remoto bloqueado con la interfaz basada en web del DRAC 5.

- "Primeros pasos para solucionar problemas de un sistema remoto"
- "Administración de alimentación en un sistema remoto"
- "Uso del registro de sucesos del sistema"
- "Cómo ver la pantalla de último bloqueo del sistema"

Primeros pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas en general en el DRAC 5:

1. ¿El sistema está encendido o apagado?
2. Si el sistema operativo está encendido, ¿se encuentra en funcionamiento, bloqueado o simplemente congelado?
3. Si está apagado, ¿se ha apagado de forma imprevista?

En el caso de sistemas bloqueados, revise la pantalla de último bloqueo (consulte "Cómo ver la pantalla de último bloqueo del sistema") y use la redirección de consola (consulte "Velocidades de actualización y resoluciones de pantalla admitidas en el sistema administrado") y la administración remota de la alimentación (consulte "Administración de alimentación en un sistema remoto") para reiniciar el sistema y observe el proceso de reinicio.

Administración de alimentación en un sistema remoto

El DRAC 5 permite realizar varias acciones de administración de la alimentación del sistema remoto, de manera que el sistema se puede recuperar después de un bloque o de algún otro suceso.

Utilice la página **Administración de la alimentación** para hacer lo siguiente:

- Ejecute un apagado ordenado por medio del sistema operativo al reiniciar, y encienda o apague el sistema.
- Consulte el **Estado de la alimentación** actual del sistema: puede ser **Encendido** o **Apagado**.

Para acceder a la página **Administración de la alimentación** desde el árbol **Sistema**, haga clic en **Sistema** y después haga clic en la ficha **Administración de la alimentación**.

NOTA: Debe tener permiso para **Ejecutar comandos de acción de servidor** para realizar acciones de administración de alimentación.

Selección de las acciones de control de alimentación desde la interfaz gráfica de usuario del DRAC 5

1. Seleccione una de las siguientes **Acciones de control del servidor**.
   - **Encender el sistema**: enciende el sistema (equivale a presionar el botón de encendido cuando el sistema está apagado).

- **Apagar el sistema**: apaga el sistema (equivale a presionar el botón de encendido cuando el sistema está encendido).
- **Restablecer el sistema**: restablece el sistema (equivale a presionar el botón de restablecimiento); la alimentación no se apaga con esta función.
- **Realizar ciclo de encendido del sistema**: apaga y después reinicia (inicio mediante suministro de energía) el sistema.

2. Haga clic en **Aplicar** para realizar la acción de administración de alimentación (por ejemplo, hacer que el sistema realice un ciclo de encendido).
3. Haga clic en el botón correspondiente de la página **Administración de la alimentación** para continuar (consulte la Tabla 15-1).

Tabla 15-1. Botones de la página de administración de la alimentación (parte superior derecha)

Botón	Acción
Imprimir	Imprime la página **Administración de la alimentación**.
Actualizar	Vuelva a cargar la página **Administración de la alimentación**.

Selección de las acciones de control de alimentación desde la CLI del DRAC 5

Use el comando `racadm serveraction` para realizar operaciones de administración de alimentación en el sistema host.

```
racadm serveraction <acción>
```

Las opciones para la cadena <*acción*> son:

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

Cómo ver la información del sistema

La página **Resumen del sistema** muestra la información sobre los siguientes componentes del sistema:

- Chasis del sistema principal
- Remote Access Controller
- Controlador de administración de la placa base

Para acceder a la información del sistema, amplíe el árbol **Sistema** y haga clic en **Propiedades**.

Chasis del sistema principal

La Tabla 15-2 y la Tabla 15-3 describen las propiedades del chasis de sistema principal.

NOTA: Para recibir la información del **Nombre de host** y el **Nombre del sistema operativo**, deberá tener instalados los servicios de DRAC 5 en el sistema administrado.

Tabla 15-2. Campos de la información del sistema

Campo	Descripción
Descripción	Descripción del sistema.
Versión del BIOS	Versión del BIOS del sistema.
Etiqueta de servicio	Número de la etiqueta de servicio del sistema.

Nombre del host	Nombre del sistema host.
Nombre del sistema operativo	El sistema operativo que se ejecuta en el sistema.

Tabla 15-3. Campos de la recuperación automática

Campo	Descripción
Acción de recuperación	Cuando se detecta un "sistema bloqueado", se puede configurar el DRAC para que ejecute una de las siguientes acciones: sin acción, restablecimiento forzado, apagar o realizar ciclo de encendido del sistema.
Cuenta regresiva inicial	El número de segundos tras la detección de un "sistema bloqueado" después de los cuales el DRAC ejecutará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Remote Access Controller

La Tabla 15-4 describe las propiedades de Remote Access Controller.

Tabla 15-4. Campos informativos del RAC

Campo	Descripción
Nombre	Nombre abreviado.
Información sobre productos	Nombre detallado.
Versión del hardware	Versión de la tarjeta Remote Access Controller o "desconocido".
Versión del firmware	Nivel de versión del firmware del DRAC 5.
Firmware actualizado	La fecha y hora en la que el firmware se actualizó por última vez.
Hora del RAC	Valor del reloj del sistema.

Controlador de administración de la placa base

La Tabla 15-5 describe las propiedades del Controlador de administración de la placa base.

Tabla 15-5. Campos informativos del BMC

Campo	Descripción
Nombre	"Controlador de administración de la placa base".
Versión de IPMI	Versión de la Interfaz de administración de plataforma inteligente (IPMI)
Número de sesiones activas posibles	Número máximo de sesiones que pueden estar activas al mismo tiempo.
Número de sesiones activas actuales	Número total de sesiones activas actuales.
Versión del firmware	Versión del firmware del BMC.
LAN activada	LAN activada o LAN desactivada

Uso del registro de sucesos del sistema

La página **Registro de sucesos del sistema** muestra los sucesos críticos del sistema que se presentan en el sistema administrado.

Para ver el registro de sucesos del sistema:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y después haga clic en **Registro de sucesos del sistema**.

La página **Registro de sucesos del sistema** muestra la gravedad del suceso y ofrece otra información según se muestra en la Tabla 15-6.

3. Haga clic en el botón correspondiente de la página **Registro de sucesos del sistema** para continuar (consulte la Tabla 15-7).

Tabla 15-6. Iconos de indicador de estado

Icono/categoría	Descripción
	Una marca de verificación verde indica una condición de estado sana (normal).
	Un triángulo amarillo que contiene un signo de admiración indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.
Fecha/Hora	La fecha y hora en la que se presentó el suceso. Si la fecha está en blanco, el suceso se presentó durante el inicio del sistema. El formato es mm/dd/aaaa hh:mm:ss, según el horario de 24 horas.
Descripción	Una breve descripción del suceso

Tabla 15-7. Botones de la página del registro de sucesos del sistema

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

Uso de la línea de comandos para ver el registro del sistema

```
racadm getsel -i
```

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

```
racadm getsel <opciones>
```

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

NOTA: Consulte "getsel" para obtener más información sobre las opciones que puede usar.

El comando **clrsel** elimina todos los registros existentes del registro de sucesos del sistema.

```
racadm clrsel
```

Uso de los registros de POST y de inicio del sistema operativo

Esta función del DRAC 5 le permite reproducir un video de imágenes detenidas de las últimas tres instancias de la prueba POST del BIOS y el inicio del sistema operativo.

Para ver los registros de captura de POST e inicio del sistema operativo:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y luego en la ficha **Captura de INICIO**.
3. Seleccione el número de registro de captura de la POST o inicio del sistema operativo.

   El video de los registros se reproducirá en una nueva pantalla.
4. Haga clic en **DETENER** para detener el video.

Cómo ver la pantalla de último bloqueo del sistema

AVISO: La función de pantalla de último bloqueo necesita que el sistema administrado tenga configurada la función **Recuperación automática** en Server Administrator. Además, asegúrese que la función **Recuperación automatizada del sistema** esté activada por medio del DRAC. Diríjase a la página **Servicios** en la ficha **Configuración** en la sección **Acceso remoto** para activar esta función.

La página **Pantalla de último bloqueo** muestra la pantalla del bloqueo más reciente, que incluye información sobre los sucesos que ocurrieron antes de que el sistema se bloqueara. La información del último bloqueo se guarda en la memoria del DRAC 5 y se puede acceder a ella de manera remota.

Para ver la página **Pantalla de último bloqueo**:

1. En el árbol **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y después haga clic en **Último bloqueo**.

La página **Pantalla de último bloqueo** tiene los siguientes botones (consulte la Tabla 15-8) en la esquina superior derecha de la pantalla:

Tabla 15-8. Botones de la página Pantalla de último bloqueo

Botón	Acción
Imprimir	Imprime la página **Pantalla de último bloqueo**.
Guardar	Abre una ventana emergente que permite guardar la pantalla de último bloqueo en el 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 recuperación automática, es posible que la **Pantalla de último bloqueo** no se capture cuando el temporizador de restablecimiento del sistema esté definido con un valor de menos de 30 segundos. Utilice Server Administrator o IT Assistant para establecer el valor del temporizador de restablecimiento del sistema en al menos 30 segundos y garantizar que la **Pantalla de último bloqueo** funcione correctamente. Para obtener información adicional, consulte "Configuración del sistema administrado para capturar la pantalla del último bloqueo".

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección explica cómo realizar las tareas relacionadas con la recuperación y solución de problemas de un DRAC 5 bloqueado.

Usted puede usar una de las siguientes herramientas para solucionar problemas del DRAC 5:

- Registro del RAC
- Consola de diagnósticos
- Registro de rastreo
- racdump
- coredump

Uso del registro del RAC

El **Registro del RAC** es un registro persistente que se mantiene en el firmware del DRAC 5. El registro contiene una lista de acciones de usuario (por ejemplo, inicio y cierre de sesión y cambios de política de seguridad) y de alertas generadas por el DRAC 5. Cuando el registro se llena, las anotaciones más antiguas se sobrescriben.

Para acceder al registro del RAC desde la interfaz de usuario del DRAC 5:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Registros** y después haga clic en **Registro del RAC**.

El **Registro del RAC** proporciona la información que aparece en la Tabla 16-1.

Tabla 16-1. Información de la página del registro del RAC

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 de dic. 16:55:47). Cuando el DRAC 5 se inicia por primera vez y no se puede comunicar con el sistema administrado, la hora se muestra como Inicio del sistema.
Origen	La interfaz que ocasionó el suceso.
Descripción	Una breve descripción del suceso y el nombre del usuario que inicio sesión en el DRAC 5.

Uso de los botones de la página de registro del RAC

La página **Registro del RAC** tiene los botones que aparecen en la Tabla 16-2.

Tabla 16-2. Botones del registro del RAC

Botón	Acción
Imprimir	Imprime la página **Registro del RAC**.

Borrar registro	Borra las anotaciones del **Registro del RAC**. **NOTA:** El botón **Borrar registro** sólo aparecerá si usted tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **Registro del RAC** en un directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en support.microsoft.com.
Actualizar	Vuelve a cargar la página **Registro del RAC**.

Utilización de la línea de comandos

Utilice el comando `getraclog` para ver las anotaciones del registro del RAC.

```
racadm getraclog -i
```

El comando **getraclog -i** muestra el número de anotaciones en el registro del DRAC 5.

```
racadm getraclog [opciones]
```

NOTA: Para obtener más información, consulte "getraclog".

Puede usar el comando `clrraclog` para borrar todas las entradas del registro del RAC.

```
racadm clrraclog
```

Uso de la consola de diagnósticos

El DRAC 5 proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la Tabla 16-3) que son similares a las herramientas que se incluyen con los sistemas equipados con Microsoft® Windows® o Linux. Por medio de la interfaz basada en web del DRAC 5 se puede acceder a las herramientas de depuración de red.

Para acceder a la página de **Consola de diagnósticos**:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Diagnósticos**.

La Tabla 16-3 describe las opciones que están disponibles en la página **Consola de diagnóstico**. Escriba un comando y haga clic en **Enviar**. Los resultados de depuración aparecen en la página **Consola de diagnóstico**.

Para actualizar la página **Consola de diagnóstico**, haga clic en **Actualizar**. Para ejecutar otro comando, haga clic en **Volver a la página de diagnósticos**.

Tabla 16-3. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del Protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
netstat	Imprime el contenido de la tabla de enrutamiento. Si se proporciona el número de interfaz opcional en el campo de texto situado a la derecha de la opción **netstat**, dicha opción imprimirá información adicional acerca del tráfico en la interfaz, uso de búfer y otra información de interfaz de red.
ping <*Dirección IP*>	Verifica que se puede acceder a la dirección IP de destino desde el DRAC 5 con el contenido de la tabla de enrutamiento actual. Se debe escribir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.

gettracelog	Muestra las anotaciones del registro de seguimiento del DRAC 5. Consulte "gettracelog" para obtener más información.

Uso del registro de rastreo

Los administradores utilizan el registro de rastreo del DRAC 5 para depurar los problemas de alertas y redes del DRAC 5.

Para acceder al registro de rastreo desde la interfaz basada en web del DRAC 5:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Diagnósticos**.
3. En el campo **Comando**, escriba el comando **gettracelog** o el comando **racadm gettracelog**.

NOTA: También puede usar este comando en la interfaz de línea de comandos. Consulte "gettracelog" para obtener más información.

El registro de rastreo recopila la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben del mismo.
- IP: rastrea los paquetes IP que se envían y reciben.

El registro de rastreo también puede contener códigos de error específicos del firmware del DRAC 5 y que se relacionan con el firmware interno del DRAC 5, no con el sistema operativo del sistema administrado.

NOTA: El DRAC 5 no mostrará mensajes de eco de ICMP (ping) con tamaños de paquete mayores de 1500 bytes.

Uso de racdump

El comando `racadm racdump` proporciona un sólo comando para obtener información sobre volcado, estado e información general sobre la placa de DRAC 5.

NOTA: Este comando sólo está disponible en las interfaces Telnet y SSH. Para obtener más información, consulte el comando "racdump".

Uso de coredump

El comando `racadm coredump` muestra información detallada sobre los problemas críticos recientes que se hayan presentado en el RAC. La información de volcado de núcleo se puede usar para diagnosticar estos problemas críticos.

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

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

El comando `racadm coredumpdelete` puede usarse para borrar los datos de **volcado de núcleo** que residan en ese momento en el RAC.

Consulte "coredump" y "coredumpdelete" para obtener más información.

Regresar a la página de contenido

Regresar a la página de contenido

Sensores

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Las sondas o sensores de hardware ayudan a supervisar los sistemas de la red de manera más eficiente, ya que permiten tomar las medidas apropiadas para evitar que se produzcan desastres tales como la inestabilidad o la caída del sistema.

Puede usar el DRAC 5 para supervisar los sensores de hardware de baterías, ventiladores, intrusión del chasis, suministros de energía, consumo de energía, temperatura y voltaje.

Sondas de baterías

Las sondas de baterías brindan información sobre el CMOS de la placa del sistema y la RAM de almacenamiento en baterías de la placa base (ROMB).

NOTA: La configuración de las baterías ROMB de almacenamiento sólo se encuentra disponible si el sistema cuenta con ROMB.

Sondas de ventiladores

Los sensores de ventiladores ofrecen la siguiente información:

- redundancia del ventilador: indica la capacidad del ventilador secundario de reemplazar al principal si no logra disipar el calor a una velocidad preestablecida.
- lista de sondas de ventiladores: la lista ofrece información sobre la velocidad de todos los ventiladores del sistema.

Sondas de intrusión del chasis

Las sondas de intrusión del chasis indican el estado del chasis, ya sea abierto o cerrado.

Sondas de suministros de energía

Las sondas de suministros de energía brindan la siguiente información:

- el estado de los suministros de energía, ya sea dentro del umbral normal o por encima de ese valor.

  NOTA: Los valores de umbral sólo pueden definirse a través de Dell™ OpenManage™ Server Administrator. Consulte la *Guía del usuario de Dell OpenManage Server Administrator* para obtener más información.

- la redundancia del suministro de energía, esto es, la capacidad del suministro de energía redundante de reemplazar al suministro principal en caso de falla.

NOTA: Si sólo existe un suministro de energía en el sistema, la sección Redundancia de suministro de energía no se visualizará.

Sondas de rendimiento del hardware

El sensor de rendimiento del hardware indica el estado de rendimiento de la unidad de procesamiento (CPU), ya sea normal o degradado. Los sensores indicarán un estado degradado cuando la CPU se haya detenido.

Sondas de supervisión de la alimentación

La supervisión de la alimentación brinda información sobre el consumo de energía en *tiempo real*, en watts y amperios. Estos datos son proporcionados al DRAC 5 a través de los sensores del firmware del controlador de administración de la placa base (BMC).

NOTA: Esta función sólo se admite en determinados sistemas Dell PowerEdge™ *x9xx* y *xx0x*.

También es posible ver una representación gráfica del consumo de energía de la última hora, día o semana a partir de la fecha actual definida en el DRAC.

Sondas de temperatura

El sensor de temperatura brinda información sobre la temperatura ambiente de la placa del sistema. Las sondas indican si el estado se encuentra dentro del umbral crítico y de advertencia preestablecido.

Sondas de voltaje

A continuación se enumeran las sondas de voltaje de uso habitual. Su sistema puede tener éstas y/ u otras sondas.

- CPU [n] VCORE
- System Board 0.9V PG
- System Board 1.5V ESB2 PG
- System Board 1.5V PG
- System Board 1.8V PG
- System Board 3.3V PG
- System Board 5V PG
- System Board Backplane PG
- System Board CPU VTT
- System Board Linear PG

Las sondas de voltaje indican si el estado se encuentra dentro de los valores de umbral crítico y de advertencia preestablecidos.

Regresar a la página de contenido

Regresar a la página de contenido

Para comenzar con el DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

El DRAC 5 permite supervisar, solucionar problemas y reparar de manera remota un sistema Dell aun cuando el sistema esté apagado. El DRAC 5 ofrece un variado conjunto de funciones, por ejemplo, la redirección de consola, los medios virtuales, el KVM virtual, la autenticación de tarjeta inteligente, etc.

La estación de administración es el sistema a partir del cual el administrador gestiona de manera remota un sistema Dell que tiene instalada una tarjeta DRAC. Los sistemas que se supervisan de esta manera se denominan sistemas administrados.

Para poder usar la tarjeta DRAC, siga estos pasos:

1. Instale la tarjeta DRAC 5 en el sistema Dell; es posible que el DRAC 5 ya esté preinstalado en el sistema, o que venga en un paquete por separado.

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

   Deberá instalar el software del DRAC 5 en la estación de administración y en el sistema administrado. Sin el software Managed System, usted no puede usar RACADM de manera local y el DRAC no puede capturar la pantalla de último bloqueo.

2. Configure las propiedades del DRAC 5, los valores de la red y los usuarios: puede configurar el DRAC 5 por medio de la utilidad de configuración de acceso remoto, la interfaz basada en web o RACADM.
3. Configure Microsoft® Active Directory® para brindar acceso al DRAC 5, lo que permite agregar y controla los privilegios de usuario del DRAC 5 para los usuarios actuales en el software Active Directory.
4. Configure la autenticación de tarjeta inteligente: la tarjeta inteligente proporciona un nivel adicional de seguridad a la empresa.
5. Configure los puntos de acceso remoto, como la redirección de consola y los medios virtuales.
6. Configure los valores de seguridad.
7. Utilice el protocolo de administración sobre la base de normas Server Management-Command Line Protocol (SM-CLP, protocolo de línea de comandos para administración de servidor) para administrar los sistemas de la red.
8. Configure las alertas para la capacidad de administración eficiente de sistemas.
9. Configure los valores de DRAC 5 Intelligent Platform Management Interface (IPMI, interfaz inteligente de administración de plataformas) para utilizar las herramientas IPMI basadas en normas con el fin de administrar los sistemas de la red.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación básica del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección proporciona información sobre cómo instalar y configurar el hardware y software del DRAC 5.

Antes de comenzar

Reúna los siguientes elementos que se incluyen con el sistema, antes de instalar y configurar el software del DRAC 5:

- Hardware de DRAC 5 (ya instalado o en el paquete opcional)
- Procedimientos de instalación del DRAC 5 (se encuentra en este capítulo)
- DVD *Dell Systems Management Tools and Documentation*

Instalación del hardware de DRAC 5

NOTA: La conexión del DRAC 5 emula una conexión de teclado USB. Como resultado, cuando reinicie el sistema no notificará si el teclado no está conectado.

Es posible que el módulo del DRAC 5 esté preinstalado en el sistema o está disponible de forma independiente en un paquete. Para comenzar con el DRAC 5 que ya está instalado en el sistema, consulte "Generalidades de la instalación y configuración del software".

Si no hay un DRAC 5 instalado en el sistema, consulte el documento *Instalación de una tarjeta de acceso remoto* que se incluye con el paquete del DRAC 5 o consulte la *Guía de instalación y solución de problemas* de la plataforma para obtener instrucciones de instalación de hardware.

NOTA: Consulte la *Guía de instalación y solución de problemas* que se incluye con el sistema para obtener información sobre cómo quitar el DRAC 5. Asimismo, revise todas las propiedades del RAC de Microsoft® Active Directory® asociadas con el DRAC 5 que retiró para garantizar la seguridad adecuada si utiliza el esquema ampliado.

Configuración del sistema para usar el DRAC 5

Para configurar el sistema para usar un DRAC 5, use la utilidad Dell™ Remote Access Configuration Utility (que anteriormente se conocía como el módulo de configuración del BMC).

Para ejecutar la utilidad Dell Remote Access Configuration Utility:

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

Si el sistema operativo comienza a cargarse antes de presionar <Ctrl><E>, espere a que el sistema termine de iniciarse y después reinicie el sistema e inténtelo de nuevo.

3. Configure el NIC.
    a. Con la tecla de flecha descendente, resalte **Selección del NIC**.
    b. Con las teclas de flecha hacia la izquierda y hacia la derecha, seleccione una de las siguientes selecciones de NIC:
        - **Dedicada**: seleccione esta opción para activar el dispositivo de acceso remoto para utilizar la interfaz dedicada de red que está disponible en el Controlador de acceso remoto (RAC). Esta interfaz no se comparte con el sistema operativo del host y enruta el tráfico de la administración hacia una red física separada, lo que permite separarlo del tráfico de aplicaciones. Esta opción sólo está disponible cuando hay una tarjeta DRAC instalada en el sistema.
        - **Compartida**: seleccione esta opción para compartir de interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos por medio de NIC 1 y NIC 2, pero transmite datos únicamente por medio de NIC 1. Si el NIC 1 falla, no se prodrá acceder al dispositivo de acceso remoto.
        - **Protección contra fallas**: seleccione esta opción para compartir de interfaz de red con el sistema operativo del host. La interfaz de red del dispositivo de acceso remoto es totalmente funcional cuando el sistema operativo del host está configurado para la formación de equipos de NIC. El dispositivo de acceso remoto recibe datos por medio de NIC 1 y NIC 2, pero transmite datos únicamente por medio de NIC 1. Si el NIC 1 falla, el dispositivo de acceso remoto utilizará el NIC 2 para todas las transmisiones de datos. El dispositivo de acceso remoto continúa usando el NIC 2 para la transmisión de datos. Si el NIC 2 falla, el dispositivo de acceso remoto vuelve a utilizar NIC 1 para todas las transmisiones de datos.
4. Configure los parámetros de LAN del controlador de red para usar DHCP o un origen de dirección IP estática.
    a. Para usar una tecla de flecha descendente, seleccione **Parámetros de LAN** y presione <Entrar>.
    b. Con las teclas de flecha hacia arriba y hacia abajo, seleccione **Origen de dirección IP**.
    c. Con las teclas de flecha hacia la derecha y hacia la izquierda, seleccione **DHCP** o **Estática**.
    d. Si seleccionó **Estática**, configure los valores de la **Dirección IP Ethernet**, la **Máscara de subred** y la **Puerta de enlace predeterminada**.
    e. Presione <Esc>.
5. Presione <Esc>.
6. Seleccione **Guardar los cambios y salir**.

El sistema se reinicia automáticamente.

NOTA: Al visualizar la interfaz Web de usuario en un sistema Dell PowerEdge™ 1900 que está configurado con un NIC, la página Configuración del NIC mostrará dos NIC (NIC1 y NIC2). Este comportamiento es normal. El sistema PowerEdge 1900 (y otros sistemas Dell que están configurados con una sola LAN incorporada a la placa base) se pueden configurar con la formación de equipos de NIC. Los modos compartidos y de equipos funcionan de manera independiente en estos sistemas.

Consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* para obtener más información sobre la utilidad Dell Remote Access Configuration Utility.

Generalidades de la instalación y configuración del software

Esta sección proporciona una descripción general del proceso de configuración del DRAC 5. Configure el DRAC 5 por medio de la interfaz basada en web, la CLI de RACADM o la consola serie, Telnet o SSH.

Para obtener más información sobre los componentes de software del DRAC 5, consulte "Instalación del software en el sistema administrado".

Instalación del software del DRAC 5

Para instalar es software del DRAC 5:

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

Configure el DRAC 5

Para configurar el DRAC 5:

1. Seleccione una de las siguientes herramientas de configuración:
    - Interfaz basada en web

- CLI de RACADM
- Consola serie, Telnet o SSH

AVISO: Si se utiliza más de una herramienta de configuración del DRAC 5 al mismo tiempo se pueden obtener resultados inesperados.

2. Configure los valores de red del DRAC 5. Consulte "Configuración de las propiedades del DRAC 5".
3. Agregue y configure usuarios del DRAC 5. Consulte "Cómo agregar y configurar usuarios del DRAC 5".
4. Configure el explorador de web para acceder a la interfaz basada en web. Consulte "Configuración de un explorador de web admitido".
5. Desactive la opción de reinicio automático de Windows®. Consulte "Desactivación de la opción de reinicio automático de Windows".
6. Actualice el firmware del DRAC 5. Consulte "Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet (sistema cliente)".
7. Acceda al DRAC 5 a través de una red. Consulte "Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet (sistema cliente)".

Instalación del software en el sistema administrado

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

Para instalar el software Managed System en el sistema administrado, utilice el DVD *Dell Systems Management Tools and Documentation*. Para obtener instrucciones sobre cómo instalar el software, consulte la *Guía de instalación rápida*.

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

NOTA: No instale el software Management Station del DRAC 5 y el software Managed System del DRAC 5 en el mismo sistema.

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

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

Instalación del software en la estación de administración

El sistema incluye el paquete Dell OpenManage Systems Management Software. Este paquete incluye, entre otras herramientas, el DVD *Dell Systems Management Tools and Documentation*, que ofrece los siguientes componentes:

- *Dell Systems Build and Update Utility*: esta utilidad de inicio agiliza la implementación y la reimplementación de los sistemas Dell y además brinda las herramientas necesarias para configurarlos y actualizarlos.
- CD *Dell Systems Console and Agent*: contiene los más recientes productos de software de administración de sistemas de Dell, como Dell OpenManage Server Administrator y productos de consola que incluyen Dell OpenManage IT Assistant.
- CD *Dell Systems Service and Diagnostics Tools*: ofrece las herramientas necesarias para configurar el sistema y proporciona los más recientes controladores optimizados para Dell, BIOS, firmware y diagnósticos para el sistema.

Para obtener información sobre la instalación del software Server Administrator, consulte la *Guía del usuario de Server Administrator*.

Configuración de la estación de administración con Red Hat Enterprise Linux (versión 4)

Dell Digital KVM Viewer requiere de configuración adicional para ejecutarse en una estación de administración con Red Hat Enterprise Linux (versión 4). Cuando instale el sistema operativo Red Hat Enterprise Linux (versión 4) en la estación de administración, realice los procedimientos siguientes:

- Cuando se le pida agregar o quitar paquetes, instale el software opcional **Legacy Software Development**. Este paquete de software incluye los componentes de software necesarios para ejecutar Dell Digital KVM Viewer en la estación de administración.

- Para garantizar que Dell Digital KVM Viewer funcione correctamente, abra los siguientes puertos en el servidor de seguridad:
  - Puerto de teclado y mouse (el puerto predeterminado es el 5900)
  - Puerto de vídeo (el puerto predeterminado es el 5901)

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

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

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

Instalación de RACADM

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

   ```
   mount /media/cdrom
   ```

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

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

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

Desinstalación de RACADM

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

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

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

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

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

Actualización del firmware del DRAC 5

Utilice uno de los métodos siguientes para actualizar el firmware del DRAC 5.

- Interfaz basada en web
- CLI de RACADM
- Dell Update Packages

Antes de comenzar

Antes de actualizar el firmware del DRAC 5 con RACADM local o Dell Update Packages, realice los siguientes procedimientos. De lo contrario, podría fallar la operación de actualización del firmware.

1. Instale y active los controladores de nodo administrado y la IPMI correspondientes.
2. Si el sistema ejecuta el sistema operativo Windows, active e inicie el servicio Instrumental de administración de Windows (WMI).
3. Si el sistema ejecuta SUSE Linux Enterprise Server (versión 10) para Intel EM64T, inicie el servicio Raw.
4. Asegúrese que la memoria flash virtual del RAC esté desmontada o que el sistema operativo u otra aplicación o usuario no la estén usando.
5. Desconecte y desmonte los medios virtuales.
6. Compruebe que el USB esté activado.

Cómo descargar el firmware del DRAC 5

Para actualizar el firmware del DRAC 5, descargue el firmware más reciente del sitio web de asistencia de Del que se encuentra en **support.dell.com** y guarde el archivo en el sistema local.

En el paquete de firmware del DRAC 5 se incluyen los siguientes componentes de software:

- Código y datos de firmware compilados del DRAC 5
- Imagen de ROM de expansión
- Interfaz basada en web, JPEG y otros archivos de datos de interfaz de usuario
- Archivos de configuración predeterminados

Utilice la página **Actualización del firmware** para actualizar el firmware del DRAC 5 a la revisión más reciente. Cuando ejecute la actualización del firmware, ésta conservará la configuración actual del DRAC 5.

Actualización del firmware del DRAC 5 mediante la interfaz basada en web

1. Abra la interfaz basada en web e inicie sesión en el sistema remoto.

   Consulte "Acceso a la interfaz basada en web".

2. En el árbol **Sistema**, haga clic en **Acceso remoto** y haga clic en la ficha **Actualizar**.
3. En la página **Actualización de firmware** en el campo **Imagen de firmware**, escriba la ruta de acceso de la imagen de firmware que descargó de **support.dell.com** o haga clic en **Examinar** para desplazarse hacia la imagen.

   NOTA: Si ejecuta Firefox, el cursor de texto no aparecerá en el campo **Imagen de firmware**.

   Por ejemplo,

   `C:\Updates\V1.0\<nombre_de_imagen>`.

   El nombre predeterminado de la imagen de firmware es **firmimg.d5**.

4. Haga clic en **Update (Actualizar)**.

   La actualización puede tardar varios minutos en terminar. Al terminar, aparecerá un cuadro de diálogo.

5. Haga clic en **OK (Aceptar)** para desconectarse y cerrar la sesión automáticamente.
6. Después de que el DRAC 5 se restablezca, haga clic en **Iniciar sesión** para iniciar sesión en el DRAC 5.

Actualización del firmware del DRAC 5 por medio de racadm

Puede actualizar el firmware del DRAC 5 mediante la herramienta racadm basada en CLI. Si ha instalado Server Administrator en el sistema administrado, utilice los comandos de racadm local para actualizar el firmware.

1. Puede descargar la imagen del firmware del DRAC 5 en el sistema administrado a través del sitio Web de asistencia técnica de Dell: **support.dell.com**.

   Por ejemplo,

   ```
   C:\downloads\firmimg.d5
   ```

2. Ejecute el siguiente comando racadm:

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

   También puede actualizar el firmware mediante comandos de racadm remota.

   Por ejemplo,

   ```
   racadm -r <dirección IP del DRAC5> U <nombre de usuario> -p <contraseña> fwupdate -p -u -d <ruta de acceso>
   ```

   donde *ruta de acceso* indica la ubicación donde se guardó **firmimg.d5** en el sistema administrado.

Actualización del firmware del DRAC 5 mediante paquetes de actualización de Dell para sistemas operativos Windows y Linux compatibles

Para descargar y ejecutar los paquetes Dell Update Packages para sistemas operativos Windows y Linux compatibles, visite el sitio Web de asistencia técnica de Dell: **support.dell.com**. Consulte la *Guía del usuario de Dell Update Package* para obtener más información.

Cómo borrar la caché del explorador

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

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

Configuración de un explorador de web admitido

Las secciones siguientes proporcionan instrucciones para configurar los exploradores de web admitidos. Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

Configuración del explorador de web para conectarse a la interfaz basada en web

Si se va a conectar a la interfaz basada en web del DRAC 5 desde una estación de administración que se conecta a la Internet por medio de un servidor proxy, debe configurar el explorador de web para acceder a la Internet desde este servidor.

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

1. Abra una ventana del explorador web.

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

Lista de dominios de confianza

Cuando se accede a la interfaz basada en web del DRAC 5 por medio del explorador de web, se le pedirá agregar la dirección IP del DRAC 5 a la lista de dominios de confianza si la dirección IP no aparece en la lista. Al terminar, haga clic en Actualizar o reinicie el explorador de web para restablecer la conexión con la interfaz basada en web del DRAC 5.

Exploradores de web de 32 bits y 64 bits

La interfaz basada en web del DRAC 5 no se admite en los exploradores de web de 64 bits. Si abre un explorador de 64 bits, accede a la página de redirección de consola e intenta instalar el complemento, el procedimiento fallará. Si este error no se reconoce y se repite este procedimiento, la página de redirección de consola se cargará aun cuando la instalación del complemento haya fallado durante el primer intento. Este problema se presenta porque el explorador de web guarda la información del complemento en el directorio del perfil aun cuando el procedimiento de instalación del complemento haya fallado. Para resolver este problema, instale y ejecute un explorador de web de 32 bits admitido e inicie sesión en el DRAC 5.

Visualización de versiones localizadas de la interfaz basada en web

Windows

La interfaz basada en web del DRAC 5 es compatible con los siguientes idiomas del sistema operativo Windows:

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

Para ver una versión traducida de la interfaz basada en web del DRAC 5 en Internet Explorer:

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

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

Linux

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

1. Abra una ventana de terminal de comandos.
2. Escriba "locale" y presione <Entrar>. Aparecerá el siguiente mensaje de salida.

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

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

   Anotación actual:

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

   Anotación actualizada:

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

6. Cierre sesión y después inicie sesión en el sistema operativo.
7. Vuelva a iniciar el DRAC 5.

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

Para ver las configuraciones avanzadas del DRAC 5, consulte "Configuración avanzada del DRAC 5".

Regresar a la página de contenido

Regresar a la página de contenido

Configuración avanzada del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección ofrece información sobre la configuración avanzada del DRAC 5. Su lectura se recomienda especialmente para los usuarios con conocimientos avanzados sobre la administración de sistemas que deseen personalizar el entorno de DRAC de acuerdo con sus necesidades específicas.

Antes de comenzar

Usted debe haber terminado la instalación y configuración básica del hardware y software del DRAC 5. Consulte "Instalación básica del DRAC 5" para obtener más información.

Configuración de las propiedades del DRAC 5

Puede configurar las propiedades del DRAC 5 properties (red, usuarios y demás) a través de la interfaz web o de RACADM.

El DRAC 5 proporciona una interfaz web y RACADM (una interfaz de línea de comandos que le permiten configurar las propiedades y los usuarios del DRAC 5, realizar tareas de administración remota y solucionar problemas de un sistema remoto (administrado). Para la administración cotidiana de sistemas, utilice la interfaz web del DRAC 5. Este capítulo contiene información sobre cómo realizar las tareas comunes de administración de sistemas con la interfaz web del DRAC 5 y ofrece vínculos a la información relacionada.

Todas las tareas de configuración de la interfaz web también se pueden realizar con RACADM.

Configuración de DRAC 5 por medio de la interfaz web de usuario

Consulte la ayuda en línea del DRAC 5 para ver información en base al contexto de cada página de la interfaz web.

Acceso a la interfaz basada en web

Para iniciar sesión en la interfaz web del DRAC 5:

1. Abra una ventana del explorador web compatible.

   Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

2. En el campo **Dirección**, escriba lo siguiente y presione <Entrar>:

   https://<*dirección IP*>

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

   https://<*dirección IP*>:<*número de puerto*>

   donde <*dirección IP*> es la dirección IP del DRAC 5 y *número de puerto* corresponde al número de puerto HTTPS.

   Aparece la ventana **Conectar** del DRAC 5.

NOTA: Si utiliza Internet Explorer versión 6 SP2 o versión 7 para conectarse a la interfaz de usuario Web del DRAC 5 y el cliente está en una red privada sin acceso a Internet, es posible que haya una demora de hasta 30 segundos. Para resolver este inconveniente:

1. Desactive el filtro de suplantación de identidad (phishing).

   https://phishingfilter.microsoft.com/faq.aspx.

2. Desactive la captura de CRL:

   a. Haga clic en **Herramientas**→ **Opciones**→ ficha **Avanzadas** → **Seguridad**.

   b. Deje sin marcar la opción **Comprobar la revocación de certificados del editor**.

Conexión

Puede iniciar sesión como usuario del DRAC 5 o como usuario de Microsoft® Active Directory®. El nombre predeterminado y la contraseña son **root** y **calvin**, respectivamente.

Antes de iniciar sesión en el DRAC 5, verifique que cuenta con permiso de **Iniciar sesión en el DRAC 5**. Consulte al administrador de red o DRAC de su organización para confirmar sus privilegios de acceso.

Para iniciar sesión:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes nombres:
   - Su nombre de usuario de DRAC 5.

     Por ejemplo, <*nombre_de_usuario*>

     En el nombre de usuario de DRAC 5 para los usuarios locales se distingue entre mayúsculas y minúsculas.
   - Su nombre de usuario de Active Directory.

     Por ejemplo, <*dominio*>\<*nombre_de_usuario*>, <*dominio*>/<*nombre_de_usuario*> o <*usuario*>@<*dominio*>.

     Algunos ejemplos de nombres de usuario de Active Directory son: **dell.com\juan_perez** o **juan_perez@dell.com**.

En los nombres de usuario de Active Directory no se distingue entre mayúsculas y minúsculas.

2. En el campo **Contraseña**, escriba la contraseña de usuario del DRAC 5 o de Active Directory.

   Este campo distingue entre mayúsculas y minúsculas.

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

Desconexión

1. En la esquina superior derecha de la ventana de la interfaz web del DRAC 5, haga clic en **Desconectar** para cerrar la sesión.
2. Cierre la ventana del explorador.

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

NOTA: El cierre del explorador sin una desconexión ordenada ocasiona que la sesión permanezca abierta hasta que se acabe el tiempo de espera. Se recomienda enfáticamente hacer clic en el botón Desconectar para terminar la sesión; de lo contrario, la sesión permanecerá activa hasta que se agote el tiempo de espera de la misma.

NOTA: Si cierra la interfaz web del DRAC 5 dentro de Microsoft Internet Explorer con el botón de cierre ("x") que se encuentra en la esquina superior derecha de la pantalla, se podría producir un error de la aplicación. Para resolver este problema, descargue la actualización acumulada de seguridad para Internet Explorer del sitio web de asistencia técnica de Microsoft, en support.microsoft.com.

Activación y configuración del DRAC 5 para utilizar una consola Telnet o serie

Los apartados siguientes proporcionan información sobre cómo activar y configurar una consola Telnet, serie o SSH en el DRAC 5.

Cómo usar el comando serie connect com2

Al utilizar el comando serie **connect com2** compruebe que lo siguientes elementos están configurados correctamente:

- El valor **Comunicación serie**→ **Puerto serie** en el programa Configuración del BIOS.
- Los valores de configuración del DRAC.

Cuando se establece una sesión Telnet en el DRAC 5 y estos valores son incorrectos, es posible que **connect com2** muestre una pantalla en blanco.

Configuración del programa de configuración del BIOS para una conexión serie en el sistema administrado

Realice los pasos siguientes para utilizar el programa Configuración del BIOS para desviar la salida a un puerto serie.

NOTA: Debe configurar el programa Configuración del sistema de manera conjunta con el comando **connect com2**.

1. Encienda o reinicie el sistema.
2. Pulse <F2> inmediatamente después de que aparezca el mensaje siguiente:

   ```
   <F2> = System Setup (F2 = Programa de configuración del sistema)
   ```

3. Desplácese hacia abajo y presione <Entrar> para seleccionar **Comunicación serie**.
4. Configure la pantalla **Comunicación serie** como se indica a continuación:

   Conector serie externo: **Dispositivo de acceso remoto**

Redirección después de inicio: **Desactivado**

5. Presione <Esc> para salir el programa Configuración de sistema y terminar la configuración del mismo.

Uso de la interfaz serie de acceso remoto

Al establecer una conexión serie con el dispositivo RAC, las siguientes interfaces están disponibles:

- Interfaz serie de IPMI. Consulte "Uso de la interfaz serie de acceso remoto de IPMI".
- Interfaz serie de RAC

Interfaz serie de RAC

RAC también admite la interfaz de consola serie (o *Consola serie de RAC*) que tiene una interfaz de línea de comandos de RAC, la cual no está definida por IPMI. Si el sistema incluye una tarjeta RAC con **Consola serie** activada, la tarjeta de RAC anulará la configuración serie de IPMI y mostrará la interfaz serie de CLI del RAC.

Para activar la interfaz de terminal serie del RAC, establezca la propiedad **cfgSerialConsoleEnable** como **1** (TRUE)(verdadero).

Por ejemplo,

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

Consulte "cfgSerialConsoleEnable (lectura/escritura)" para obtener más información.

La Tabla 4-1 muestra la configuración de la interfaz serie.

Tabla 4-1. Configuración de la interfaz serie

Modo IPMI	Consola serie del RAC	Interfaz
Básico	Desactivado	Modo básico
Básico	Activado	CLI del RAC
Terminal	Desactivado	Modo de terminal de IPMI
Terminal	Activado	CLI del RAC

Configuración de Linux para la redirección de la consola serie durante el inicio

Los pasos a continuación son específicos para GRand Unified Bootloader (GRUB) de Linux. Será necesario hacer cambios similares si se utiliza otro cargador de inicio.

NOTA: Cuando configure la ventana de emulación de cliente VT100, configure la ventana o aplicación que esté mostrando la consola redirigida en 25 filas x 80 columnas a fin de garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo **/etc/grub.conf** como se indica a continuación:

1. Localice las secciones General Setting (Configuración general) dentro del archivo y agregue las siguientes dos líneas:

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. Agregue dos opciones a la línea de núcleo:

```
kernel ..... console=ttyS1,57600
```

3. Si el archivo **/etc/grub.conf** contiene una directiva splashimage, inserte un carácter de comentario al inicio de la línea para anularla.

La Tabla 4-2 contiene un ejemplo del archivo **/etc/grub.conf** que muestra los cambios que se describen en este procedimiento.

Tabla 4-2. Archivo de ejemplo: /etc/grub.conf

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root= /dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0 console= ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Cuando modifique el archivo **/etc/grub.conf**, aplique las siguientes directrices:

1. Desactive la interfaz gráfica de GRUB y utilice la interfaz de texto; de lo contrario, la pantalla de GRUB no aparecerá en la redirección de consola del RAC. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con splashimage.

2. Para activar varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión en serie del RAC, agregue la siguiente línea a todas las opciones:

   ```
   console=ttyS1,57600
   ```

   La Tabla 4-2 muestra la cadena console=ttyS1,57600 ya agregada a la primera opción solamente.

Activación del inicio de sesión en la consola después de inicio

Modifique el archivo **/etc/inittab** según se indica a continuación:

Agregue una nueva línea para configurar agetty en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

La Tabla 4-3 muestra un archivo de ejemplo con la nueva línea.

Tabla 4-3. Archivo de ejemplo: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)

#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifique el archivo **/etc/securetty** según se indica a continuación:

Agregue una nueva línea con el nombre del tty serie para COM2:

```
ttyS1
```

La Tabla 4-4 muestra un archivo de ejemplo con la nueva línea.

Tabla 4-4. Archivo de ejemplo: /etc/securetty

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Activación de la consola serie, Telnet o SSH del DRAC 5

La consola serie, Telnet o SSH se puede activar de manera local o remota.

Activación de la consola serie, Telnet o SSH de manera local

NOTA: Para poder realizar los pasos de esta sección, usted (el usuario actual), usted debe tener permiso para Configurar el DRAC 5.

Para activar la consola serie, Telnet o SSH desde el sistema administrado, escriba los siguientes comandos de RACADM local en una petición de comandos:

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

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

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

Activación de la consola serie, Telnet o SSH de manera remota

Para activar la consola serie, Telnet o SSH de manera remota, escriba los siguientes comandos de **RACADM** remota en una petición de comandos:

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial -o cfgSerialConsoleEnable 1
```

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial -o cfgSerialTelnetEnable 1
```

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial -o cfgSerialSshEnable 1
```

NOTA: Si utiliza Internet Explorer versión 6 SP2 o versión 7 para conectarse a un sistema administrado que está en una red privada sin acceso a Internet, es posible que haya una demora de hasta 30 segundos durante el uso de los comandos RACADM remotos.

Uso del comando RACADM para configurar los valores de la consola Telnet y serie

Este apartado contiene los pasos para definir los valores de configuración predeterminados de la redirección de consola serie, Telnet o SSH.

Para configurar los valores, escriba el comando **config** de RACADM con el grupo, la propiedad y los valores de propiedad adecuados para el valor que desea configurar.

Puede escribir los comandos de RACADM de manera local o remota. Al utilizar los comandos de RACADM de manera remota, debe incluir el nombre de usuario, la contraseña y la dirección IP del DRAC 5 del sistema administrado.

Uso de RACADM de manera local

Para escribir los comandos de RACADM de manera local, escriba el comando siguiente en una petición de comando del sistema administrado:

```
racadm config -g <grupo> -o <propiedad> <valor>
```

Para ver una lista de las propiedades, escriba el comando siguiente en una petición de comandos del sistema administrado:

```
racadm getconfig -g <grupo>
```

Uso de RACADM de manera remota

Para usar los comandos de RACADM de manera remota, escriba el comando siguiente en una petición de comandos de una estación de administración:

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g <grupo> -o <propiedad> <valor>
```

Asegúrese que el servidor web esté configurado con una tarjeta DRAC 5 antes de utilizar RACADM de manera remota. De lo contrario, RACADM agotará el tiempo de espera y aparecerá el siguiente mensaje:

```
No se puede conectar al RAC en la dirección IP que se especificó.
```

Para activar el servidor web por medio de Secure Shell (SSH), Telnet o RACADM local, escriba el siguiente comando en una petición de comandos de una estación de administración:

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

Visualización de valores de configuración

La Tabla 4-5 contiene las acciones y los comandos relacionados para mostrar los valores de configuración. Para ejecutar los comandos, abra una petición de comandos en el sistema administrado, escriba el comando y presione <Entrar>.

Tabla 4-5. Visualización de valores de configuración

Acción	Comando
Muestra una lista de los grupos disponibles.	racadm getconfig -h
Muestra la configuración actual de un grupo específico.	racadm getconfig -g *<grupo>* Por ejemplo, para mostrar una lista de toda la configuración del grupo **cfgSerial**, escriba el siguiente comando: racadm getconfig -g cfgSerial

Muestra la configuración actual de un grupo específico de manera remota.	racadm -u <*usuario*> -p *<contraseña>* -r *<dirección IP del DRAC 5>* getconfig -g cfgSerial Por ejemplo, para visualizar una lista de toda la configuración del grupo **cfgSerial** de manera remota, escriba lo siguiente: racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

Configuración del número de puerto de Telnet

Escriba el comando a continuación para cambiar el número de puerto de Telnet en el DRAC 5.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <número del nuevo puerto>
```

Uso de una consola telnet o serie

Puede ejecutar los comandos serie que se muestran en la Tabla 4-19 de manera remota con RACADM o desde la petición de comandos de la consola serie, Telnet o SSH.

Cómo iniciar sesión en el DRAC 5

Después de haber configurado el software emulador de terminal de estación de administración y el BIOS del nodo administrado, realice los pasos siguientes para iniciar sesión en el DRAC 5:

1. Conéctese al DRAC 5 con el software de emulación de terminal de la estación de administración.
2. Escriba el nombre de usuario del DRAC 5 y presione <Entrar>.

Ha iniciado sesión en el DRAC 5.

Inicio de una consola de texto

Después de haber iniciado sesión en el DRAC 5 a través del software de terminal de la estación de administración con Telnet o SSH, usted puede desviar la consola de texto del sistema administrado por medio de **connect com2**, que es un comando de Telnet/SSH. Sólo se admite un cliente de **connect com2** a la vez.

Para conectar la consola de texto del sistema administrado, abra una petición de comandos de DRAC 5 (por medio de una sesión de Telnet o SSH) y escriba:

```
connect com2
```

Desde una sesión serie, puede conectar la consola serie del sistema administrado si presiona <Esc><Mayús><Q>. Esta combinación conecta el puerto serie del sistema administrado directamente al puerto COM2 de los servidores y no pasa por el DRAC 5. Para volver a conectar el DRAC 5 al puerto serie, presione <Esc><Mayús><9>. Las velocidades en baudios del puerto COM2 del nodo administrado y del puerto serie del DRAC 5 deben ser idénticas.

El comando `connect -h com2` muestra el contenido del búfer de historial de la conexión serie antes de esperar información proveniente del teclado o nuevos caracteres provenientes del puerto serie.

NOTA: Cuando se utiliza la opción **-h**, el tipo de emulación de terminal de cliente y servidor (ANSI o VT100) debe ser idéntico; de lo contrario, los mensajes de salida pueden ser ilegibles. Además, defina el número de filas de terminal de cliente como **25**.

El tamaño predeterminado (y máximo) del búfer de historial es de 8192 caracteres. Puede asignar un número menor a este valor con el comando:

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

Configuración de los modos serie y terminal

Configuración de la conexión serie de RAC e IPMI

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. Configurar los valores de conexión serie de IPMI.

   Consulte la Tabla 4-6 para ver una descripción de los valores de la conexión serie de IPMI.
4. Configurar los valores de conexión serie de RAC.

   Consulte la Tabla 4-7 para ver una descripción de los valores de la conexión serie de RAC.
5. Haga clic en **Aplicar cambios**.
6. Haga clic en el botón adecuado de la página **Configuración serie** para continuar. Consulte la Tabla 4-8 para ver una descripción de los valores de la página de configuración de la conexión serie.

Tabla 4-6. Configuración de la conexión serie de IPMI

Valor	Descripción
Configuración del modo de conexión	• Modo básico de conexión directa: Modo básico de conexión serie de IPMI • Modo de terminal de conexión directa: Modo de terminal de conexión serie de IPMI
Velocidad en baudios	Establece la velocidad de los datos. Seleccione **9600 bps**, **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.
Control de flujo	• Ninguno: Control de flujo de hardware apagado • RTS/CTS: Control de flujo de hardware encendido
Límite del nivel de privilegios del canal	• Administrador • Operador • Usuario

Tabla 4-7. Configuración de la conexión serie de RAC

Valor	Descripción
Activado	Activa o desactiva la consola serie de RAC. Seleccionada=activada; deseleccionada=desactivada
Número máximo de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema.
Tiempo de espera	La cantidad máxima de segundos de línea disponible antes de que la línea se desconecte. El rango es de 60 a 1920 segundos. El valor predeterminado es de 300 segundos. Utilice 0 segundos para desactivar la función de tiempo de espera.
Redirección activada	Activa o desactiva la redirección de consola. Seleccionada=activada; deseleccionada=desactivada
Velocidad en baudios	La velocidad de los datos en el puerto serie externo. Los valores son **9600 bps**, **28,8 kbps**, **57,6 kbps** y **115,2 kbps**. El valor predeterminado es de **57,6 kbps**.
Tecla Escape	Especifica la tecla <Esc>. El valor predeterminado son los caracteres ^\.
Tamaño del búfer de historial	El tamaño del búfer de historial de la conexión serie, que guarda los últimos caracteres que se escribieron en la consola. El valor máximo y predeterminado es 8192 caracteres.
Comando de inicio de sesión	La línea de comando del DRAC que se ejecutará ante un inicio de sesión válido.

Tabla 4-8. Valores de la página de configuración de la conexión serie

Botón	Descripción
Imprimir	Imprime la página **Configuración de la conexión serie**.
Actualizar	Actualiza la página **Configuración de la conexión serie**.
Aplicar cambios	Aplica los cambios de la conexión serie de RAC e IPMI.

Configuración del modo de terminal	Abre la página **Configuración del modo de terminal**.

Configuración del modo de terminal

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. En la página **Configuración de la conexión serie**, haga clic en **Configuración del modo de terminal**.
4. Defina la configuración del modo de terminal.

   Consulte la Tabla 4-9 para ver una descripción de la configuración del modo de terminal.
5. Haga clic en **Aplicar cambios**.
6. Haga clic en el botón correspondiente de la página **Configuración del modo de terminal** para continuar. Consulte la Tabla 4-10 para ver una descripción de los botones de la página de configuración del modo de terminal.

Tabla 4-9. Configuración del modo de terminal

Valor	Descripción
Edición de línea	Activa o desactiva la edición de línea.
Control de eliminación	Selecciona una de las siguientes opciones: • **El BMC genera un carácter <retroceso><espacio><retroceso> cuando se recibe <retroceso> o <supr>**. • **El BMC genera un carácter <supr> cuando se recibe <retroceso> o <supr>**.
Control del eco	Activa o desactiva el eco.
Control del protocolo de enlace	Activa o desactiva el protocolo de enlace.
Nueva secuencia de línea	Selecciona **Ninguno**, **<CR-LF>**, **<NULO>**, **<CR>**, **<LF-CR>** o **<LF>**.
Introducir una nueva secuencia de línea	Seleccione **<CR>** o **<NULO>**.

Tabla 4-10. Botones de la página de configuración del modo de terminal

Botón	Descripción
Imprimir	Imprime la página **Configuración del modo de terminal**.
Actualizar	Actualiza la página **Configuración del modo de terminal**.
Regresar a la configuración del puerto serie	Regresa a la página **Configuración del puerto serie**.
Aplicar cambios	Aplica los cambios de la configuración del modo de terminal.

Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet (sistema cliente)

El sistema administrado ofrece acceso entre el DRAC 5 y el puerto serie del sistema para permitir que usted encienda, apague o restablezca el sistema administrado y tenga acceso a los registros.

La consola serie está disponible en el DRAC 5 a través del conector serie externo del sistema administrado. Sólo un sistema cliente serie (estación de administración) puede estar activo a la vez. Las consolas Telnet y SSH están disponibles en el DRAC 5 por medio de los modos del DRAC (consulte "Modos del DRAC"). Se pueden conectar hasta cuatro sistemas cliente Telnet y cuatro clientes SSH a la vez. La conexión de management station con la consola Telnet o serie del sistema administrado requiere del software de emulación de terminal de estación de administración. Consulte "Configuración del software de emulación de terminal de la estación de administración" para obtener más información.

Los apartados siguientes explican cómo conectar la estación de administración con el sistema administrado por medio de los métodos siguientes:

- Un puerto serie externo del sistema administrado a través del software de terminal y un cable nulo de módem o DB-9
- Una conexión de Telnet con software de terminal a través del NIC del DRAC 5 del sistema administrado o del NIC agrupado y compartido

---

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

Para acceder al sistema administrado con una consola de texto serie, conecte un cable de módem nulo DB-9 al puerto COM del sistema administrado. No todos los cables DB-9 tienen la distribución de patillas/señales necesaria para esta conexión. El cable DB-9 de esta conexión debe cumplir las especificaciones que se muestran en la Tabla 4-11.

NOTA: El cable DB-9 también se puede usar para la redirección de consola de texto de BIOS.

Tabla 4-11. Distribución de patillas necesaria para el cable de módem nulo DB-9

Nombre de señal	Patilla DB-9 (patilla de servidor)	Patilla DB-9 (patilla de estación de trabajo)
FG (protección de tierra)	–	–
TD (transmisión de datos)	3	2
RD (recepción de datos)	2	3
RTS (solicitud de envío)	7	8
CTS (listo para envío)	8	7
SG (señal de tierra)	5	5
DSR (conjunto de datos listo)	6	4
CD (detección de transportador)	1	4
DTR (terminal de datos listo)	4	1 y 6

Configuración del software de emulación de terminal de la estación de administración

El DRAC 5 admite una consola de texto Telnet o serie de una estación de administración que ejecuta uno de los siguientes tipos de software de emulación de terminal:

- Linux Minicom en Xterm
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve
- Linux Telnet en Xterm
- Microsoft® Telnet

Realice los pasos en los apartados siguientes para configurar el tipo del software de terminal. Si está usando Microsoft Telnet, no se requiere la configuración.

Configuración de Linux Minicom para la emulación de consola serie

Minicom es la utilidad de acceso a puerto serie de Linux. Los pasos siguientes son válidos para configurar Minicom versión 2.0. Otras versiones de Minicom pueden diferenciarse ligeramente, pero requieren los mismos valores básicos. Utilice la información en "Valores de Minicom necesarios para la emulación de consola serie" para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0 para emulación de la consola serie

NOTA: Para garantizar que el texto se muestre correctamente, Dell recomienda que se utilice una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece el sistema Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en la petición de comandos.
2. En la ventana de Xterm, lleve la flecha del mouse a la esquina inferior derecha de la ventana y cambie el tamaño de la ventana a 80 x 25.
3. Si no tiene un archivo de configuración de Minicom, vaya al siguiente paso.

Si tiene un archivo de configuración de Minicom, escriba `minicom <nombre` del archivo de configuración de *Minicom*> y luego vaya al paso 17.

4. En la petición de comandos de Xterm, escriba `minicom -s`.
5. Seleccione **Serial Port Setup** (Configuración de puerto serie) y pulse <Intro>.
6. Presione <a> y seleccione el dispositivo serie correspondiente (por ejemplo, **/dev/ttyS0**).
7. Presione <e> y establezca la opción **Bps/Par/Bits** en **57600 8N1**.
8. Presione <f> y establezca **Control de flujo de hardware** en **Sí** y **Control de flujo de software** en **No**.
9. Para salir del menú **Configuración del puerto serie**, presione <Entrar>.
10. Seleccione **Módem y marcación** y presione <Entrar>.
11. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco.
12. Presione <Entrar> para guardar cada uno de los valores en blanco.
13. Cuando se hayan borrado todos los campos especificados, presione <Entrar> para salir del menú **Configuración de parámetros y marcación de módem**.
14. Seleccione **Guardar configuración como nombre_de_config** y presione <Entrar>.
15. Seleccione **Salir de Minicom** y presione <Entrar>.
16. En la petición del intérprete de comandos, escriba `minicom <nombre del archivo de configuración de Minicom>`.
17. Para ampliar la ventana de Minicom a 80 x 25, arrastre la esquina de la misma.
18. Presione <Ctrl+a>, <z>, <x> para salir de Minicom.

NOTA: Si utiliza Minicom para la redirección de consola de texto serie para configurar el BIOS del sistema administrado, se recomienda activar el color en Minicom. Para activar el color, escriba el comando siguiente: `minicom -c on`

Compruebe que la ventana Minicom muestre una petición de comandos como `[DRAC 5\root]#`. Cuando la petición de comandos aparezca, la conexión se habrá establecido satisfactoriamente y usted estará listo para conectarse a la consola del sistema administrado por medio del comando serie **connect**.

Valores de Minicom necesarios para la emulación de consola serie

Utilice la Tabla 4-12 para configurar cualquier versión de Minicom.

Tabla 4-12. Valores de Minicom para emulación de consola serie

Descripción del valor	Valor necesario
Bps/Par/Bits	57600 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Marcación de módem y configuración de parámetros	Borre los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco
Tamaño de ventana	80 x 25 (para cambiar el tamaño, arrastre la esquina de la ventana)

Configuración de HyperTerminal para la redirección de consola serie

HyperTerminal es la utilidad de acceso de puerto serie de Microsoft Windows. Para establecer el tamaño de la pantalla de consola correctamente, utilice HyperTerminal Private Edition versión 6.3 de Hilgraeve.

Para configurar HyperTerminal para la redirección de consola serie:

1. Inicie el programa HyperTerminal.
2. Escriba un nombre para la nueva conexión y haga clic en **OK (Aceptar)**.
3. Junto a **Conectar usando:**, seleccione el puerto COM en la estación de administración (por ejemplo, COM2) al que ha conectado el cable de módem nulo DB-9 y haga clic en **OK (Aceptar)**.
4. Configure los valores del puerto COM según se muestra en la Tabla 4-13.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Archivo** → **Propiedades** y después haga clic en la ficha **Configuración**.
7. Defina la **Id. de la terminal de Telnet:** como **ANSI**.

8. Haga clic en **Configuración de terminal** y establezca **Filas de pantalla** en **26**.
9. Establezca **Columnas** en **80** y haga clic en **OK (Aceptar)**.

Tabla 4-13. Configuración del puerto COM de la estación de administración

Descripción del valor	Valor necesario
Bits por segundo	57600
Bits de datos	8
Paridad	Ninguno
Bits de parada	1
Control de flujo	Hardware

La ventana de HyperTerminal muestra una petición de comandos como `[DRAC 5\root]#`. Cuando la petición de comandos aparezca, la conexión se habrá establecido satisfactoriamente y usted estará listo para conectarse a la consola del sistema administrado por medio del comando serie **connect com2**.

Configuración de Linux XTerm para la redirección de consola de Telnet

Utilice las siguientes directricies al ejecutar los pasos de esta sección:

- Al utilizar el comando **connect com2** mediante una consola Telnet para visualizar las pantallas de configuración del sistema, establezca el tipo de terminal en **ANSI** en el programa Configuración del sistema y para la sesión Telnet.
- Para garantizar que el texto se muestre correctamente, Dell recomienda que se utilice una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece el sistema Linux.

Para ejecutar Telnet con Linux:

1. Inicie una nueva sesión de Xterm.

   En la petición de comandos, escriba `xterm &`
2. Con la flecha del mouse, haga clic en la esquina inferior derecha de la ventana XTerm y cambie el tamaño de la ventana a 80 x 25.
3. Conéctese al DRAC 5 en el sistema administrado.

   En la petición de Xterm, escriba `telnet <`*`dirección IP del DRAC 5`*`>`

Activación de telnet de Microsoft para redirección de consola telnet

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

1. Active **Telnet** en **Servicios de componentes de Windows**.
2. Conéctese al DRAC 5 en la estación de administración.

   Abra un indicador de comandos, escriba lo siguiente y pulse <Intro>:

   `telnet <`*`dirección IP`*`>:<`*`número de puerto`*`>`

   donde *`dirección IP`* es la dirección IP del DRAC 5 y el *`número de puerto`* es el número de puerto de Telnet (si se está usando un puerto nuevo).

Configuración de la tecla de retroceso para la sesión de Telnet

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

Para configurar los clientes Telnet de Microsoft para que utilicen la tecla <Retroceso>:

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

   ```
   telnet
   ```

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

   ```
   set bsasdel
   ```

   Aparece el mensaje siguiente:

   ```
   Backspace will be sent as delete.
   ```

   (El retroceso se procesará como eliminación.)

Para configurar una sesión de Telnet de Linux a fin de que utilice la tecla <Retroceso>:

1. Abra una petición de comandos y escriba:

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

   ```
   telnet
   ```

Uso de una consola telnet o serie

Los comandos **serie** y **telnet**, y de CLI de RACADM, se pueden escribir en una consola serie o Telnet y se pueden ejecutar en el servidor de manera remota o local. La CLI de RACADM local está instalada para uso exclusivo del usuario "root".

Ejecución de Telnet con Windows XP o Windows 2003

Si la estación de administración ejecuta Windows XP o Windows 2003, es posible que se experimente un problema con los caracteres en las sesiones Telnet del DRAC 5. Este problema se puede presentar como un inicio de sesión que se bloquea y en el que la tecla de retorno no responde y no aparece la petición de contraseña.

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

Ejecución de Telnet con Windows 2000

Si la estación de administración ejecuta Windows 2000, no se podrá acceder a la configuración del BIOS al presionar la tecla <F2>. Para resolver este problema, use el cliente Telnet que se incluye en la descarga gratuita recomendada de los servicios de Windows para UNIX® 3.5 de Microsoft. Vaya a **www.microsoft.com/downloads/** y busque "*Windows Services for UNIX 3.5*." (Servicios de Windows para UNIX 3.5).

Uso de Secure Shell (SSH)

Es crucial que los dispositivos del sistema y la administración de dispositivos estén seguros. Los dispositivos incorporados y conectados son el centro medular de muchos procesos comerciales. Si estos dispositivos son vulnerables, la empresa puede estar en riesgo, lo que requiere de nuevas exigencias de seguridad al software de administración de dispositivos de CLI (interfaz de línea de comandos).

Secure Shell (SSH) es una sesión de línea de comandos que incluye las mismas capacidades que una sesión de Telnet, pero con mayor seguridad. El DRAC 5 admite SSH versión 2 con autenticación de contraseña. SSH se activa en el DRAC 5 cuando usted instala o actualiza el firmware del DRAC 5.

Se puede usar PuTTY u OpenSSH en la estación de administración para conectarse al DRAC 5 del sistema administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente Secure Shell envía un mensaje de error. El texto del mensaje está en función del cliente y el DRAC 5 no lo controla.

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

Sólo se admiten cuatro sesiones SSH a la vez. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se decribe en "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5".

Para activar SSH en el DRAC 5, escriba:

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

Para cambiar el puerto SSH, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>
```

Para obtener más información sobre las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5".

La implementación de SSH del DRAC 5 admite varios esquemas de criptografía, según se muestra en la Tabla 4-14.

Tabla 4-14. Esquemas de criptografía

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

NOTA: No se admite SSHv1.

Configuración de valores de red del DRAC 5

AVISO: Si cambia la configuración de red del DRAC 5, es posible que se desconecte la conexión de red actual.

Configure los valores de red del DRAC 5 con una de las herramientas siguientes:

- Interfaz web: consulte "Configuración de la tarjeta de interfaz de red del DRAC 5"
- CLI de RACADM: consulte "cfgLanNetworking"
- Utilidad de configuración de acceso remoto de Dell: consulte "Configuración del sistema para usar el DRAC 5"

NOTA: Si va a instalar el DRAC 5 en un entorno de Linux, consulte "Instalación de RACADM".

Acceso al DRAC 5 por medio de una red

Depués de configurar el DRAC 5, usted puede acceder de manera remota el sistema administrado pr medio de una de las interfaces siguientes:

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

La Tabla 4-15 describe cada interfaz del DRAC 5.

Tabla 4-15. Interfaces del DRAC 5

Interfaz	Descripción
Interfaz basada en web	Ofrece acceso remoto al DRAC 5 por medio de una interfaz gráfica de usuario. La interfaz web está integrada en el firmware del DRAC 5 y se accede a ella por medio de la interfaz de NIC a partir de un explorador de web compatible de la estación de administración. Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

RACADM	Ofrece acceso remoto al DRAC 5 por medio de una interfaz de línea de comandos. RACADM utiliza la dirección IP del sistema administrado para ejecutar comandos de RACADM (opción de capacidad remota de racadm [-r]).
	
	NOTA: La capacidad remota de racadm sólo se admite en las estaciones de administración. Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.
	
	NOTA: Al utilizar la capacidad remota de racadm, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de racadm que involucran operaciones de archivos, por ejemplo:
	
	`racadm getconfig -f <nombre de archivo>`
	
	`o bien:`
	
	`racadm sslcertupload -t 1 -f c:\cert\cert.txt subcomandos`

Consola Telnet	Proporciona acceso al puerto de RAC del servidor y las interfaces de administración de hardware por medio del NIC del DRAC 5 y admite comandos serie y RACADM, por ejemplo, los comandos **powerdown**, **powerup**, **powercycle** y **hardreset**. **NOTA:** Telnet es un protocolo no seguro que transmite todos los datos —incluso las contraseñas— en texto simple. Cuando transmita información confidencial, utilice la interfaz SSH.
Interfaz SSH	Proporciona las mismas capacidades que la consola Telnet a través de de una capa de transporte cifrada que brinda mayor seguridad.
Interfaz IPMI	Brinda acceso a las funciones de administración básicas del sistema remoto por medio del DRAC 5. La interfaz incluye IPMI mediante LAN, IPMI mediante conexión serie y Conexión serie mediante LAN. Para obtener más información, consulte la *Guía del usuario del controlador de*

	administración de la placa base de Dell OpenManage.

NOTA: El nombre de usuario predeterminado del DRAC 5 es root y la contraseña predeterminada es calvin.

Puede acceder a la interfaz basada en web del DRAC 5 mediante la tarjeta de interfaz de red del DRAC 5 con un explorador de web admitido, o bien, mediante Server Administrator o IT Assistant.

Para obtener una lista de exploradores de web admitidos, consulte la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

Para acceder a la interfaz de acceso remoto del DRAC 5 por medio de Server Administrator, ejecute Server Administrator. En el árbol de sistema que se encuentra en el panel a la izquierda de la página de inicio de Server Administrator, haga clic en **Sistema** → **Chasis del sistema principal** → **Controlador de acceso remotor**. Para obtener más información, consulte la guía del usuario de Server Administrator.

Configuración de la tarjeta de interfaz de red del DRAC 5

Configuración de los valores de LAN de IPMI y de red

NOTA: Para realizar los pasos siguientes se debe tener permiso para **Configurar el DRAC 5**.

NOTA: La mayoría de los servidores DHCP requieren un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el DRAC 5) debe proporcionar este testigo durante la negociación de DHCP. Para los RAC, el DRAC 5 proporciona la opción de identificador de cliente a través de un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

NOTA: Si el DRAC del sistema administrado se configura como **Compartido** o como modo **Compartido con protección contra fallas** y el DRAC está conectado a un conmutador con STP (Protocolo de árbol de expansión) activado, los clientes de la red experimentarán un retraso de 20 a 30 segundos en la conexión cuando el estado del vínculo LOM de la estación de administración cambie durante la convergencia de STP.

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Red**.
3. En la página **Configuración de red**, configure los valores de la tarjeta de interfaz de red del DRAC 5.

   La Tabla 4-16 y la Tabla 4-17 describen la **Configuración de red** y la **Configuración de IPMI** en la página de **Configuración de la red**.
4. Cuando termina, haga clic en **Aplicar cambios**.
5. Haga clic en el botón correspondiente de la página **Configuración de la red** para continuar. Consulte el apartado Tabla 4-18.

Tabla 4-16. Configuración de red

Valor	Descripción
Selección de NIC	Muestra el modo seleccionado de NIC (**Dedicado**, **Compartido con protección contra fallas** o **Compartido**). El valor predeterminado es **Dedicado**.
MAC Address	Muestra la dirección MAC del DRAC 5.
Activar NIC	Activa la tarjeta de interfaz de red del DRAC 5 y los controles restantes en este grupo. El valor predeterminado es **Activada**.
Usar DHCP (Para la dirección IP de la tarjeta de interfaz de red)	Activa Dell OpenManage™ Server Administrator para obtener la dirección IP de la tarjeta de interfaz de red a partir del servidor de Protocolo de configuración de host dinámico (DHCP). Si selecciona la casilla, se desactivarán los controles **Dirección IP estática**, **Puerta de enlace estática**, y **Máscara de subred estática**. La configuración predeterminada es **Desactivada**.
Dirección IP estática	Especifica o edita la dirección IP estática de la tarjeta de interfaz de red del DRAC 5. Para cambiar este valor, deseleccione la casilla **Usar DHCP (para dirección IP de la tarjeta de interfaz de red)**.
Puerta de enlace estática	Especifica o edita la puerta de enlace estática de la tarjeta de interfaz de red del DRAC 5. Para cambiar este valor, deseleccione la casilla **Usar DHCP (para dirección IP de la tarjeta de interfaz de red)**.
Máscara de subred estática	Especifica o edita la máscara de subred estática de la tarjeta de interfaz de red del DRAC 5. Para cambiar este valor, deseleccione la casilla **Usar DHCP (para dirección IP de la tarjeta de interfaz de red)**.
Usar DHCP para obtener direcciones de servidor DNS	Obtiene las direcciones primaria y secundaria del servidor DNS a partir del servidor DHCP en vez de utilizar los valores estáticos.

	La configuración predeterminada es **Desactivada**.
Servidor DNS preferido estático	Utiliza la dirección IP del servidor DNS primario sólo cuando la opción **Usar DHCP para obtener direcciones de servidor DNS no está seleccionada**.
Servidor DNS alternativo estático	Utiliza la dirección IP del servidor DNS secundario cuando la opción **Usar DHCP para obtener direcciones de servidor DNS no está seleccionada**. Si no tiene un servidor DNS alternativo, puede introducir la dirección IP 0.0.0.0.
Registrar el DRAC en el DNS	1 = Registra el nombre del DRAC 5 en el servidor DNS. La configuración predeterminada es **Desactivada**.
Nombre del DRAC de DNS	Muestra el nombre del DRAC 5 sólo cuando **Registrar el DRAC 5 en el DNS** está seleccionado. El nombre predeterminado del DRAC 5 es RAC-etiqueta de servicio, donde etiqueta de servicio es el número de la etiqueta de servicio del servidor Dell (por ejemplo, RAC-EK00002).
Usar DHCP para el nombre del dominio de DNS	Utiliza el nombre de dominio DNS predeterminado. Cuando la casilla no está seleccionada y se selecciona la opción **Registrar el DRAC 5 en el DNS**, usted puede modificar el nombre de dominio DNS en el campo **Nombre de dominio DNS**. La configuración predeterminada es **Desactivada**.
Nombre del dominio DNS	El nombre de dominio DNS predeterminado es **MYDOMAIN**. Cuando la casilla **Usar DHCP para el nombre de dominio DNS** está seleccionada, esta opción se deshabilita y no se podrá modificar este campo.
Negociar automáticamente	Determina si el DRAC 5 establece automáticamente el **Modo dúplex** y la **Velocidad de red** comunicándose con el enrutador o concentrador más cercano (**Activado**) o permite que usted establezca el **Modo dúplex** y la **Velocidad de red** manualmente (**Desactivado**).
Velocidad de red	Configura la velocidad de red en 100 Mb o 10 Mb para coincidir con el entorno de red. Esta opción no está disponible si **Negociación automática** se ha establecido como **Activada**.
Modo dúplex	Configura el modo dúplex como completo o medio para coincidir con el entorno de red. Esta opción no está disponible si **Negociación automática** se ha establecido como **Activada**.

Tabla 4-17. Configuración de la LAN IPMI

Valor	Descripción
Activar IPMI en la LAN	Activa el canal de LAN de IPMI.
Límite del nivel de privilegios del canal	Configura el nivel de privilegio máximo del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: Administrador, Operador o Usuario.
Clave de cifrado	Configura el formato de caracteres de la clave de cifrado: 0 a 20 caracteres hexadecimales (no se permiten espacios vacíos). El valor predeterminado es **00000000000000000000**.
Activar identificación de VLAN	Activa la Id. de VLAN. Si se activa, sólo se aceptará el tráfico de la Id. de VLAN que coincida.
Identificación de VLAN	El campo de Id. de VLAN de campos de 802.1g.
Prioridad	El campo Prioridad de campos de 802.1g.

Tabla 4-18. Botones de la página de configuración de la red

Botón	Descripción
Imprimir	Imprime la página **Configuración de la red**
Actualizar	Vuelve a cargar la página **Configuración de la red**
Configuración avanzada	Muestra la página **Seguridad de la red**.
Aplicar cambios	Guarda los cambios realizados en la configuración de red. **NOTA:** Si se hacen cambios en la configuración de la dirección IP de la tarjeta de interfaz de red se cerrarán todas las sesiones de usuarios y estos deberán volver a conectarse a la interfaz web del DRAC 5 con la nueva configuración de dirección IP. Todos los demás cambios requerirán que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Para obtener más información, consulte "Establecimiento de la configuración de la seguridad de red por medio de la interfaz gráfica de usuario del DRAC 5".

Uso de RACADM de manera remota

NOTA: Configure la dirección IP en el DRAC 5 antes de usar la capacidad remota de racadm. Para obtener más información sobre cómo configurar el DRAC 5 y una lista de los documentos relacionados, consulte "Instalación básica del DRAC 5".

RACADM proporciona una opción de capacidad remota (**-r**) que le permite conectarse al sistema administrado y ejecutar subcomandos de **racadm** desde una consola remota o una estación de administración. Para usar la capacidad remota, usted necesita un nombre de usuario (opción **-u**) y una contraseña (opción **-p**) válidos, así como la dirección IP del DRAC 5.

NOTA: Si el sistema desde el que está accediento al sistema remoto no tiene un certificado de DRAC en el almacén predeterminado de certificados, aparecerá un mensaje cuando escriba un comando de racadm.

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio

Ejecución continua. Utilice la opción -S para que racadm detenga la ejecución al producirse errores relacionados con certificados.)
```

racadm continúa ejecutando el comando. No obstante, si utiliza la opción –S, racadm detendrá la ejecución del comando y mostrará el siguiente mensaje:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

EORROR: Unable to connect to RAC at specified IP address

(Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio

Racadm detiene la ejecución del comando.

ERROR: no es posible establecer conexión con el RAC en la dirección IP especificada)
```

NOTA: La capacidad remota de racadm sólo se admite en las estaciones de administración. Para obtener más información, consulte la matriz de compatibilidad de software de los sistemas Dell que se encuentra en el sitio web de asistencia de Dell en support.dell.com.

NOTA: Al utilizar la capacidad remota de racadm, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de racadm que involucran operaciones de archivos, por ejemplo:

```
racadm getconfig -f <nombre de archivo>
```

O bien:

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

Sinopsis de RACADM

```
racadm -r <dirección IP del RAC> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del RAC> <subcomando> <opciones del subcomando>
```

Por ejemplo,

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del RAC se cambió a un puerto personalizado distinto del puerto predeterminado (443), se debe utilizar la sintaxis siguiente:

```
racadm -r <dirección IP del RAC>:<puerto> -u <nombre_de_usuario> -p <contraseña> <subcomando> <opciones del subcomando>
```

```
racadm -i -r <dirección IP del RAC>:<puerto> <subcomando> <opciones del subcomando>
```

Opciones de RACADM

La Tabla 4-19 muestra una lista de las opciones del comando **racadm**.

Tabla 4-19. Opciones del comando racadm

Opción	Descripción
-**r <Direc_IP_de_RAC>** -**r <Direc_IP_de_RAC>:<**número de puerto**>**	Especifica la dirección IP remota del controlador. Utilice :<número de puerto> si el número de puerto del DRAC 5 no es el puerto predeterminado (443)
-**i**	Indica a **racadm** que pregunte interactivamente al usuario el nombre de usuario y la contraseña.
-**u <Nombre_de_usuario>**	Especifica el nombre de usuario que se usa para autentificar la transacción del comando. Si se usa la opción **-u**, se debe usar la opción **-p** y la opción **-i** (interactiva) no se permite.
-**p <contraseña>**	Especifica la contraseña usada para autentificar la transacción del comando. Si se usa la opción **-p**, la opción **-i** no se permite.
-S	Indica que **racadm** debe verificar si existen errores por certificados no válidos. **racadm** detiene la ejecución del comando y muestra un mensaje de error si detecta un certificado no válido.

Activación y desactivación de la capacidad de racadm remota

NOTA: Se recomienda ejecutar estos comandos en el sistema local.

La capacidad de racadm remota está activada de manera predeterminada. Si se desactiva, escriba el siguiente comando de racadm para activarla:

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

Para desactivar la capacidad remota, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

Subcomandos de RACADM

La Tabla 4-20 proporciona la descripción de cada uno de los subcomandos de **racadm** que se puede ejecutar en RACADM. Para ver una lista detallada de los subcomandos de racadm que incluye la sintaxis y las anotaciones válidas, consulte "Generalidades del subcomando RACADM".

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

```
racadm help
```

Tabla 4-20. Subcomandos de RACADM

Comando	Descripción
help	Muestra una lista de los subcomandos del DRAC 5.
help <subcomando>	Muestra la descripción de uso del subcomando especificado.
arp	Muestra el contenido de la tabla de ARP. Las anotaciones del ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la pantalla de último ASR (bloqueo) (la última pantalla azul).
clrraclog	Borra el registro del DRAC 5. Sólo se hace una anotación para indicar el usuario y la hora en la que se borró el registro.
config	Configura el RAC.
getconfig	Muestra las propiedades actuales del RAC.
coredump	Muestra el el último volcado de núcleo del DRAC 5.
coredumpdelete	Elimina el volcado de núcleo que está guardado en el DRAC 5.
fwupdate	Ejecuta o muestra el estado de las actualizaciones del firmware del DRAC 5.
getssninfo	Muestra información sobre las sesiones activas.
getsysinfo	Muestra información general del DRAC 5 y del sistema.
getractime	Muestra la hora del DRAC 5.
ifconfig	Muestra la configuración IP actual del RAC.
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.
ping	Verifica que se puede acceder a la dirección IP de destino desde el DRAC 5 con el contenido de la tabla de enrutamiento actual.
setniccfg	Establece la configuración IP para el controlador.
getniccfg	Muestra la configuración IP actual del controlador.
getsvctag	Muestra las etiquetas de servicio.
racdump	Vacía el estado del DRAC 5 y la información de estado para fines de depuración.
racreset	Restablece el DRAC 5.
racresetcfg	Restablece la configuración predeterminada del DRAC 5.
serveraction	Realiza operaciones de administración de energía en el sistema administrado.
getraclog	Muestra el registro del RAC.
clrsel	Borra las anotaciones del registro de sucesos del sistema.
gettracelog	Muestra las anotaciones del registro de seguimiento del DRAC 5. Si se utiliza con -i, el comando muestra la cantidad de anotaciones del registro de rastreo del DRAC 5.
sslcsrgen	Genera y descarga la CSR de SSL.
sslcertupload	Carga un certificado de CA o un certificado de servidor en el DRAC 5.
sslcertdownload	Descarga un certificado de CA.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el DRAC 5.
testemail	Obliga al DRAC 5 a enviar un mensaje de correo electrónico de prueba a través del NIC del DRAC 5 para comprobar la configuración de correo electrónico.
testtrap	Obliga al DRAC 5 a enviar una captura SNMP de prueba a través del NIC del DRAC 5 para comprobar la configuración de capturas.
vmdisconnect	Obliga el cierre de la conexión de medios virtuales.
vmkey	Restablece el tamaño predeterminado de la memoria flash virtual (16 MB).

Preguntas frecuentes sobre los mensajes de error de RACADM

Después de realizar un restablecimiento del DRAC 5 (con el comando racadm racreset), ejecuto un comando y aparece el siguiente mensaje:

racadm <nombre del comando> Transporte: ERROR: (RC=-1)

¿Qué significa este mensaje?

Debe esperar a que termine el restablecimiento del DRAC 5 antes de ejecutar otro comando.

Cuando uso los comandos y subcomandos de racadm, recibo mensajes de error que no entiendo.

Es posible que reciba uno o más de los siguientes errores cuando use los comandos y subcomandos de **racadm**:

- Mensajes de errores locales: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc.
- Mensajes de errores remotos: problemas tales como una dirección IP, nombre de usuario o contraseña incorrectos.

Cuando ejecuto el comando ping con la dirección IP del DRAC desde mi sistema y luego cambio mi tarjeta DRAC 5 entre los modos Dedicado y Compartido durante la respuesta del comando ping, no recibo respuesta.

Borre la tabla ARP en el sistema.

Configuración de varias tarjetas DRAC 5

Con RACADM, usted puede configurar una o más tarjetas DRAC 5 con propiedades idénticas. Al consultar una tarjeta DRAC 5 específica por medio de la Id. de grupo y la Id. de objeto de la misma, RACADM crea el archivo de configuración **racadm.cfg** a partir de la información obtenida. Si exporta el archivo a una o más tarjetas DRAC 5, podrá configurar los controladores con propiedades idénticas en un periodo mínimo.

NOTA: Algunos archivos de configuración contienen información única de DRAC 5 (por ejemplo, la dirección IP estática) que se debe modificar antes de exportar el archivo a otras tarjetas DRAC 5.

Para configurar varias tarjetas DRAC 5, realice los siguientes procedimientos:

1. Utilice RACADM para consultar el DRAC 5 de destino que contiene la configuración adecuada.

   NOTA: El archivo .cfg generado no contiene contraseñas de usuario.

   Abra una petición de comandos y escriba:

   ```
   racadm getconfig -f miarchivo.cfg
   ```

   NOTA: La redirección de la configuración de RAC hacia un archivo por medio de **getconfig -f** sólo se admite con las interfaces local y remota de RACADM.

2. Modifique el archivo de configuración con un editor de textos simple (opcional).
3. Utilice el nuevo archivo de configuración para modificar un RAC de destino.

   En la petición de comandos, escriba:

   ```
   racadm config -f myfile.cfg
   ```

4. Restablezca el RAC de destino que fue configurado.

   En la petición de comandos, escriba:

   ```
   racadm reset
   ```

El subcomando **getconfig -f racadm.cfg** solicita la configuración del DRAC 5 y genera el archivo **racadm.cfg**. Si se requiere, puede configurar el archivo con otro nombre.

Puede usar el comando **getconfig** para ejecutar las siguientes acciones:

- Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice)
- Mostrar todas las propiedades de configuración de usuario por nombre de usuario

El subcomando **config** carga la información en otros DRAC 5. Utilice **config** para sincronizar la base de datos de usuario y contraseña con Server Administrator.

El usuario asigna el nombre al archivo de configuración inicial, **racadm.cfg**. En el siguiente ejemplo, el archivo de configuración se denomina **miarchivo.cfg**. Para crear este archivo, escriba lo siguiente en la petición de comandos:

```
racadm getconfig -f miarchivo.cfg
```

AVISO: Se recomienda que edite este archivo con un editor de textos simple. La utilidad racadm utiliza un analizador de textos ASCII. Los elementos de formato confunden al analizador y esto puede dañar la base de datos de racadm.

Creación de un archivo de configuración del DRAC 5

El archivo de configuración del DRAC 5 <nombre_de_archivo>**.cfg** se utiliza con el comando `racadm config -f <nombre_de_archivo>.cfg`. Puede usar el archivo de configuración para crear un archivo de configurcaión (parecido a un archivo **.ini**) y configurar el DRAC 5 a partir de este archivo. Usted puede usar cualquier nombre de archivo y el archivo no requiere una extensión **.cfg** (aunque en este apartado nos refiramos al mismo con dicha extensión).

El archivo **.cfg** se puede:

- Crear
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg`
- Obtener a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y después modificarse

NOTA: Consulte "getconfig" para obtener información sobre el comando **getconfig**.

El archivo **.cfg** se analiza primero para verificar que los nombres de grupo y de objeto sean válidos y que se sigan algunas reglas simples de sintaxis. Los errores se señalan con el número de la línea en la que se detectó el error y un mensaje simple explica el problema. El archivo completo se analiza para confirmar que sea correcto y se muestran todos los errores. Si se encuentra un error en el archivo **.cfg** no se transmitirán comandos de escritura al DRAC 5. El usuario debe corregir *todos* los errores antes de que pueda realizar cualquier configuración. La opción **-c** se puede usar en el subcomando **config**, que verifica sólo la sintaxis y no realiza operaciones de escritura en el DRAC 5.

Utilice las siguientes directrices al crear un archivo **.cfg**:

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

  El analizador lee en todos los índices del DRAC 5 para dicho grupo. Los objetos dentro del grupo son simples modificaciones realizadas al configurar el DRAC 5. Si un objeto modificado representa un nuevo índice, el índice se crea en el DRAC 5 durante la configuración.

- No se puede especificar el índice que se desea en un archivo **.cfg**.

  Los índices se pueden crear y eliminar, por lo que con el tiempo el grupo se puede fragmentar con índices usados y no usados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método permite tener flexibilidad al momento de agregar anotaciones indexadas en las que usted no necesita hacer coincidencias exactas de índice entre todos los RAC que se administran. Se agregan nuevos usuarios al primer índice disponible. Un archivo **.cfg** que se analiza y se ejecuta correctamente en un DRAC 5 podría no ejecutarse correctamente en otro si todos los índices están llenos y se tiene que agregar un nuevo usuario.

- Utilice el subcomando **racresetcfg** para configurar todas las tarjetas DRAC 5 con propiedades idénticas.

  Utilice el subcomando **racresetcfg** para restablecer los valores predeterminados originales del DRAC 5 y después ejecutar el comando `racadm config -f <nombre_de_archivo>.cfg` . Asegúrese que el archivo **.cfg** tenga todos los objetos, usuarios, índices y demás parámetros requeridos.

AVISO: Use el subcomando **racresetcfg** para restablecer la base de datos y los valores predeterminados originales de la configuración de la tarjeta de interfaz de red del DRAC 5 y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas del análisis

- Todas las líneas que comienzan con '#' son tratadas como comentarios.

  Una línea de comentario debe comenzar en la columna uno. Un carácter "#" en cualquier otra columna se trata como un carácter "#".

  Algunos parámetros de módem pueden incluir caracteres # en la cadena. No se requiere un carácter de escape. Se recomienda generar un archivo **.cfg** a partir de un comando `racadm getconfig -f <nombre del archivo>.cfg` y luego realizar un comando `racadm config -f <nombre del archivo>.cfg` para un DRAC 5 diferente, sin agregar caracteres de escape.

  Ejemplo:

  ```
  #

  # This is a comment (Esto es un comentario)

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<# de inicio de módem, no es un comentario>
  ```

- Todas las anotaciones de grupo deben estar rodeadas por los caracteres "**[**"y "**]**".

  El carácter "**[**" de inicio que denota un nombre de grupo *debe* comenzar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en "Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5".

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

  Ejemplo:

  ```
  [cfgLanNetworking] -{nombre de grupo}

  cfgNicIpAddress=143.154.133.121 {nombre de objeto}
  ```

- Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor.

  Se ignorarán los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de una cadena de valores se mantienen sin modificación. Los caracteres a la derecha del símbolo "=" se tomará, tal cual (por ejemplo, un segundo "=" o un símbolo "#", "[", "]", etc.). Todos estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

  Consulte el ejemplo en el punto anterior.

- El analizador de **.cfg** ignora una anotación de objeto de índice.

  El usuario no puede especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva anotación en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <nombre del archivo>.cfg` coloca un comentario delante de los objetos de índice, lo que permite al usuario ver los comentarios incluidos.

  NOTA: Usted puede crear un grupo indexado manualmente, con el siguiente comando:
  `racadm config -g <nombre_de_grupo> -o <objeto anclado> -i <indice de 1 a 16> <nombre de ancla único>`

- La línea de un grupo indexado no se puede eliminar de un archivo **.cfg**.

El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

```
racadm config -g <nombre_de_grupo> -o <nombre_de_objeto> -i <índice de 1 a 16> ""
```

NOTA: Una cadena NULA (es decir, dos caracteres "") indica al DRAC 5 que elimine el índice del grupo especificado.

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

```
racadm getconfig -g <nombre_de_grupo> -i <índice de 1 a 16>
```

- Para grupos indexados, el ancla de objeto debe ser el primer objeto después del par de corchetes ([ ]). Los siguientes son ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]

cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
```

Si escribe `racadm getconfig -f <mi_ejemplo>.cfg`, el comando creará un archivo .**cfg** para la configuración actual del DRAC 5. Este archivo de configuración se puede usar como ejemplo y como punto de partida para su archivo **.cfg** exclusivo.

Modificación de la dirección IP del DRAC 5

Al modificar la dirección IP del DRAC 5 en el archivo de configuración, elimine todas las anotaciones innecesarias de **<**variable**>**=**valor**. Sólo permanece la etiqueta del grupo variable real con "[" y "]", incluso las dos anotaciones de **<**variable**>**=**valor** que pertenecen al cambio de dirección IP.

Por ejemplo,

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

```
#

# Object Group "cfgLanNetworking"
```

```
#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

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

cfgNicGateway=10.35.9.1
```

El comando **racadm config -f mi_archivo.cfg** analiza el archivo e identifica todos los errores por número de línea. Un archivo correcto actualizará las anotaciones adecuadas. Además, usted puede usar el mismo comando **getconfig** que se usó en el ejemplo anterior para confirmar la actualización.

Utilice este archivo para descargar cambios que abarcan toda la empresa o para configurar nuevos sistemas en la red.

NOTA: "Anchor" es un término interno y no se debe utilizar en el archivo.

Configuración de las propiedades de red del DRAC 5

Para generar una lista de las propiedades disponibles de red, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

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

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

Los comandos brindan la misma funcionalidad de configuración que la opción ROM al momento de arranque cuando se pide que presione <Ctrl><e>. Para obtener más información sobre cómo configurar las propiedades de red con la opción ROM, consulte "Configuración de las propiedades de red del DRAC 5".

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 establece como **0**, se desactivará la LAN del DRAC 5 aun cuando DHCP esté activado.

Modos del DRAC

El DRAC 5 se puede establecer en uno o tres modos:

- Dedicado
- Compartido
- Compartido con protección contra fallas

La Tabla 4-21 ofrece una descripción de cada modo.

Tabla 4-21. Configuraciones de la tarjeta de interfaz de red del DRAC 5

Modo	Descripción
Dedicado	El DRAC utiliza su propia tarjeta de interfaz de red (conector RJ-45) y la dirección MAC del BMC para el tráfico de red.
Compartido	El DRAC utiliza LOM1 de Broadcom en el plano.
Compartido con protección contra fallas	El DRAC utiliza LOM1 y LOM2 de Broadcom como equipo para protección contra fallas. El equipo utiliza la dirección MAC del BMC.

Preguntas más frecuentes

Al acceder a la interfaz basada en web del DRAC 5, aparece una advertencia de seguridad que indica que el nombre de host del certificado de SSL no coincide con el nombre de host del DRAC 5.

El DRAC 5 incluye un certificado de servidor predeterminado de DRAC 5 para garantizar la seguridad de red de las funciones de la interfaz web y de racadm remota. Cuando se usa este certificado, el explorador de web muestra una advertencia de seguridad porque el certificado predeterminado se emitió para el **Certificado predeterminado de DRAC 5**, que no coincide con el nombre de host del DRAC 5 (por ejemplo, la dirección IP).

Para resolver este asunto de seguridad, cargue un certificado de servidor del DRAC 5 que haya sido creado para la dirección IP de este último. Al generar la solicitud de firma de certificado (CSR) que se usará para emitir el certificado, asegúrese que el nombre común (CN) de la solicitud tenga la misma dirección IP del DRAC 5 (por ejemplo, 192.168.0.120) o el nombre DNS registrado del DRAC.

Para garantizar que la CSR coincide con el nombre DNS registrado del DRAC:

1. En el árbol **Sistema**, haga clic en **Acceso remoto**.

2. Haga clic en la ficha **Configuración** y haga clic en **Red**.
3. En la página **Configuración de red**:
    a. Seleccione la casilla **Registrar el DRAC en el DNS** .
    b. En el campo **Nombre DNS del DRAC**, introduzca el nombre del DRAC.
4. Haga clic en **Aplicar cambios**.

Consulte "Cómo hacer que las comunicaciones del DRAC 5 sean seguras por medio de certificados digitales y de SSL" para obtener más información sobre cómo producir CSR y cómo emitir certificados.

¿Por qué no están disponibles racadm remota y los servicios basados en web después de un cambio de propiedad?

Es posible que los servicios de RACADM remota y la interfaz basada en web tarden un poco en estar disponibles después de restablecer el servidor web del DRAC 5.

El servidor web del DRAC 5 se restablece después de los siguientes casos:

- Cuando la configuración de red o las propiedades de seguridad de la red se cambian mediante la interfaz web de usuario del DRAC 5
- Cuando la propiedad **cfgRacTuneHttpsPort** cambia (incluso cuando un comando config -f <archivo_de_config> la cambia)
- Cuando se utiliza **racresetcfg**
- Cuando el DRAC 5 se restablece
- Cuando se carga un nuevo sertificado de servidor SSL

¿Por qué mi servidor DNS no registra mi DRAC 5?

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

Al acceder a la interfaz web del DRAC 5, aparece una advertencia de seguridad que indica que el certificado SSL fue emitido por una autoridad de certificados (CA) que no es confiable.

El DRAC 5 incluye un certificado de servidor predeterminado de DRAC 5 para garantizar la seguridad de red de las funciones de la interfaz web y de racadm remota. Este certificado no fue emitido por una CA confiable. Para resolver este asunto de seguridad, cargue un certificado de servidor de DRAC 5 que haya sido emitido por una autoridad de certificados (CA) confiable (por ejemplo, Thawte o Verisign). Consulte "Cómo hacer que las comunicaciones del DRAC 5 sean seguras por medio de certificados digitales y de SSL" para obtener más información acerca de la emisión de certificados.

Regresar a la página de contenido

Regresar a la página de contenido

Cómo agregar y configurar usuarios del DRAC 5

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

- Uso de la utilidad RACADM para configurar usuarios del DRAC 5

Para administrar el sistema con el DRAC 5 y mantener la seguridad del sistema, cree usuarios únicos con permisos administrativos específicos (o *autoridad en base a funciones*). Para una mayor seguridad, también puede configurar alertas que se envían por correo electrónico a usuarios específicos cuando se presente un suceso específico en el sistema.

Para agregar y configurar usuarios del DRAC 5:

NOTA: Debe tener permiso de configurar el DRAC 5 para poder realizar los pasos siguiente.

1. Expanda el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Usuarios**.

   Aparecerá la página **Usuarios**, que incluye el **Estado**, **Nombre de usuario, Privilegio de RAC**, **Privilegio de LAN de IPMI**, **Privilegio de conexión serie de IPMI** y **Comunicación serie en la LAN** de cada uno de los usuarios.
3. En la columna **Id. de usuario**, haga clic en un número de identificación de usuario.
4. En la página **Menú principal de usuario**, puede configurar usuarios, cargar un certificado de usuario, ver un certificado de usuario existente, cargar un certificado de una autoridad de certificados de confianza o ver un certificado de CA de confianza.

   Si selecciona **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página de configuración de usuario. Para obtener más información, consulte el apartado paso 5.

   Consulte la Tabla 5-1 si selecciona las opciones en la sección **Configuración de tarjeta inteligente**.
5. En la página **Configuración de usuario**, configure las propiedades y los privilegios de usuario.

   La Tabla 5-2 describe la configuración **General** para definir un nombre de usuario y contraseña nuevos o existentes de DRAC.

   La Tabla 5-3 describe los **Privilegios de usuario de IPMI** necesarios para configurar los privilegios de LAN del usuario.

   La Tabla 5-4 describe los **Permisos de grupo de usuarios** para los valores de configuración **Privilegios de usuario de IPMI** y **Privilegios de usuario de DRAC**.

   La Tabla 5-5 describe los permisos de **Grupo de DRAC**. Si agrega un privilegio de usuario de DRAC al administrador, al usuario avanzado o al usuario invitado, el **Grupo de DRAC** cambiará a grupo **Personalizado**.
6. Cuando termina, haga clic en **Aplicar cambios**.
7. Haga clic en el botón correspondiente de la página **Configuración de usuario** para continuar. Consulte el apartado Tabla 5-6.

Tabla 5-1. Opciones en la sección de configuración de tarjeta inteligente

Opción	Descripción
Cargar certificado de usuario	Permite cargar el certificado de usuario en el DRAC e importarlo al perfil del usuario.
Ver certificado de usuario	Muestra la página de certificado de usuario que se cargó en el DRAC.
Cargar certificado de CA de confianza	Permite cargar el certificado de CA de confianza en el DRAC e importarlo al perfil del usuario.
Ver certificado de CA de confianza	Muestra el certificado de CA de confianza que se cargó en el DRAC. El certificado de CA de confianza lo emite la CA que está autorizada para emitir certificados para usuarios.

Tabla 5-2. Propiedades generales

Propiedad	Descripción
Identificación de usuario	Especifica uno de los 16 números de identificación de usuario predefinidos. Si va a editar información del usuario "root", este campo es estático. Usted no puede editar el nombre del usuario "root".
Activar el usuario	Activa el usuario para que tenga acceso al DRAC 5. Cuando está deseleccionada, no se puede cambiar el nombre de usuario.
Nombre de usuario	Especifica un nombre de usuario del DRAC 5 con hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único. **NOTA:** Los nombres de usuario en el DRAC 5 local no pueden incluir los caracteres **/** (diagonal) o **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Cambiar contraseña	Activa los campos **Nueva contraseña** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Especifica o edita la contraseña del usuario del DRAC 5.
Confirmar nueva contraseña	Requiere que vuelva a escribir la contraseña del usuario del DRAC 5 para su confirmación.

Tabla 5-3. Privilegios del usuario de IPMI

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

Tabla 5-4. Privilegios de usuario del DRAC

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

Tabla 5-5. Permisos de grupo del DRAC

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

Tabla 5-6. Botones de la página de configuración de usuario

Botón	Acción
Imprimir	Imprime la página **Configuración de la red**
Actualizar	Actualiza la página **Configuración de la red**
Volver a la página de usuarios	Regresa a la **página de usuarios**.
Aplicar cambios	Guarda los cambios realizados en la configuración de red.

Uso de la utilidad RACADM para configurar usuarios del DRAC 5

NOTA: Se debe haber iniciado sesión como usuario **root** para ejecutar los comandos de RACADM en un sistema remoto con Linux.

La interfaz web del DRAC 5 es la forma más rápida de configurar un DRAC 5. Si prefiere configuración mediante línea de comandos o secuencias de comandos o si necesita configurar varios DRAC 5, utilice RACADM, que se instala con los agentes de DRAC 5 en el sistema administrado.

Para configurar varios DRAC 5 con valores de configuración idénticos, realice uno de los siguientes procedimientos:

- Use los ejemplos de RACADM en esta sección como guía para crear un archivo de procesamiento en lote de comandos **racadm** y después ejecute el archivo de procesamiento en lote en cada sistema administrado.
- Cree un archivo de configuración de DRAC 5 según se describe en "Generalidades del subcomando RACADM" y ejecute el subcomando **racadm config** en cada sistema administrado por medio del mismo archivo de configuración.

Antes de comenzar

Puede configurar hasta 16 usuarios en la base de datos de propiedades del DRAC 5. Antes de activar manualmente un usuario de DRAC 5, verifique si ya existen usuarios. Si va a configurar un nuevo DRAC 5 o si ejecuta el comando **racadm racresetcfg**, el único usuario actual será `root` con la contraseña `calvin`. El subcomando **racresetcfg** restablece los valores predeterminados originales del DRAC 5.

AVISO: Tenga cuidado cuando utilice el comando **racresetcfg**, pues con éste se restablecen los valores predeterminados de *todos* los parámetros de configuración. Todos los cambios anteriores se perderán.

NOTA: Los usuarios se pueden activar o desactivar posteriormente. En consecuencia, es posible que un usuario tenga un número de índice distinto en cada DRAC 5.

Para verificar si existe un usuario, escriba el comando siguiente en la petición de comandos:

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

O bien:

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

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

NOTA: También puede escribir racadm getconfig -f <mi_archivo.cfg> y ver o editar el archivo **mi_archivo.cfg**, que incluye todos los parámetros de configuración del DRAC 5.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

Si el objeto **cfgUserAdminUserName** no tiene un valor, el número de índice que indica el objeto **cfgUserAdminIndex** está disponible para su uso. Si hay un nombre después del signo "=", el nombre de usuario tomará ese índice.

NOTA: Cuando agrega o borra un usuario manualmente con el subcomando **racadm config**, *debe especificar* el índice con la opción -**i**. Note que el objeto **cfgUserAdminIndex** mostrado en el ejemplo anterior contiene un carácter '#'. Asimismo, si utiliza el comando **racadm config** -**f racadm.cfg** para especificar el número de grupos/objetos a escribir, el índice no se podrá especificar. Se agrega un nuevo usuario al primer índice disponible. Este comportamiento permite tener más flexibilidad al configurar varios DRAC 5 con los mismos valores.

Cómo agregar un usuario de DRAC 5

Para agregar un nuevo usuario a la configuración del RAC, se pueden usar unos cuantos comandos básicos. En general, realice los siguientes procedimientos:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los privilegios de usuario.
4. Active el usuario.

Ejemplo

El siguiente ejemplo describe cómo agregar un nuevo usuario de nombre "Juan" con la contraseña "123456" y privilegios de inicio de sesión en el RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Para verificarlo, use uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig –g cfgUserAdmin –i 2
```

Cómo quitar un usuario de DRAC 5

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

El ejemplo siguiente ilustra la sintaxis de comando que se puede usar para eliminar un usuario de RAC:

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

Una cadena nula de dos caracteres de comillas ("") indica al DRAC 5 que elimine la configuración de usuario en el índice especificado y que restablezca los valores predeterminados originales de fábrica de configuración del usuario.

Comprobación de las alertas por correo electrónico

La función de alertas por correo electrónico del RAC permite que los usuarios reciban alertas por correo electrónico cuando se presenta un suceso crítico en el sistema administrado. El ejemplo a continuación muestra cómo probar la función de envío de alertas por correo electrónico para garantizar que el RAC pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Compruebe que los valores de **SMTP** y **Alerta por correo electrónico** estén configurados antes de probar la función de envío de alertas por correo electrónico. Consulte "Configuración de alertas por correo electrónico" para obtener más información.

Comprobación de la función de alertas de captura SNMP del RAC

La función de alertas de captura SNMP del RAC permite que las configuraciones del detector de capturas SNMP para recibir capturas para sucesos de sistema que se presenten en el sistema administrado.

El siguiente ejemplo muestra la manera en la que un usuario puede probar la función de alertas de capturas SNMP del RAC.

```
racadm testtrap -i 2
```

Antes de probar la función de alertas de capturas SNMP del RAC, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Consulte las descripciones de los comandos "**testtrap**" y "**testemail**" para configurar estos valores.

Activación de un usuario de DRAC 5 con permisos

Para activar un usuario con permisos administrativos específicos (autoridad en base a funciones), encuentre primero un índice de usuario disponible por medio de los pasos de la sección "Antes de comenzar". Posteriormente, escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña.

NOTA: Consulte la Tabla B-2 para ver una lista de los valores válidos de máscara de bits para los privilegios de usuario específicos. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios habilitados.

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

Regresar a la página de contenido

Regresar a la página de contenido

Uso del DRAC 5 con Microsoft Active Directory

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Un servicio de directorio se usa para mantener una base de datos común de toda la información necesaria para controlar a usuarios, equipos, impresoras, etc., en una red. Si la empresa ya utiliza el software de servicio Microsoft® Active Directory®, usted puede configurar el software para que proporcione acceso al DRAC 5, lo que permite agregar y controlar privilegios de usuario del DRAC 5 a los usuarios actuales en el software Active Directory.

NOTA: El uso de Active Directory para reconocer usuarios del DRAC 5 se admite en los sistemas operativos Microsoft Windows® 2000, Windows Server® 2003 y Windows Server 2008.

Prerrequisitos para activar la autenticación de Active Directory para el DRAC 5

Para usar la función de autenticación de Active Directory del DRAC 5, usted ya debe haber instalado una infraestructura de Active Directory. La autenticación de Active Directory del DRAC 5 admite la autenticación entre varios árboles en un solo bosque. Consulte "Configuración compatible de Active Directory" para obtener información sobre la configuración compatible de Active Directory con respecto al nivel de función de dominio, los grupos, los objetos, etc.

Consulte el sitio Web de Microsoft para obtener información sobre cómo configurar una infraestructura de Active Directory si aún no tiene una.

El DRAC 5 utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para autenticarse de manera segura en Active Directory, por lo tanto, usted también necesitará una PKI integrada en la infraestructura de Active Directory.

Consulte el sitio Web de Microsoft para obtener más información sobre la configuración de PKI.

Para autenticar correctamente todos los controladores de dominio, también necesitará habilitar la Capa de conexión segura (SSL) en todos los controladores de dominio. Consulte "Activación de SSL en un controlador de dominio" para obtener información más específica.

Mecanismos de autenticación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de usuario del DRAC 5 por medio de dos métodos: usted puede usar una solución de *esquema estándar*, que utiliza únicamente los objetos de grupo de Active Directory o puede usar la solución de *esquema ampliado*, que Dell ha personalizado para incluir los objetos de Active Directory definidos por Dell. Para obtener más información sobre estas soluciones, consulte las secciones siguientes.

Cuando se utiliza Active Directory para configurar el acceso al DRAC 5, se debe elegir entre la solución de esquema ampliado y el esquema estándar.

Las ventajas de usar la solución de esquema estándar son:

- No se requiere la ampliación del esquema porque el esquema estándar utiliza únicamente objetos de Active Directory.
- La configuración en Active Directory es sencilla.

Las ventajas de usar la solución de esquema ampliado son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Máxima flexibilidad al configurar acceso de usuarios en las distintas tarjetas DRAC 5 con distintos niveles de privilegios.

Generalidades del esquema estándar de Active Directory

Como se muestra en la Figura 6-1, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en el DRAC 5. En Active Directory, se utiliza un objeto de grupo estándar como grupo de funciones. El usuario que tiene acceso al DRAC 5 pertenecerá al grupo de funciones. Para dar a este usuario acceso a una tarjeta DRAC 5 específica, se deben configurar un nombre de grupo de funciones y el nombre de dominio en la tarjeta DRAC 5 específica. A diferencia de la solución de esquema ampliado, el nivel de privilegios y la función se definen en cada tarjeta DRAC 5 y no en Active Directory. En cada DRAC 5 se pueden configurar y definir hasta cinco grupos de funciones. La Tabla 6-12 muestra el nivel de privilegios de los grupos de funciones, en tanto la Tabla 6-1 muestra la configuración predeterminada del grupo de funciones.

Figura 6-1. Configuración del DRAC 5 con Microsoft Active Directory y el esquema estándar

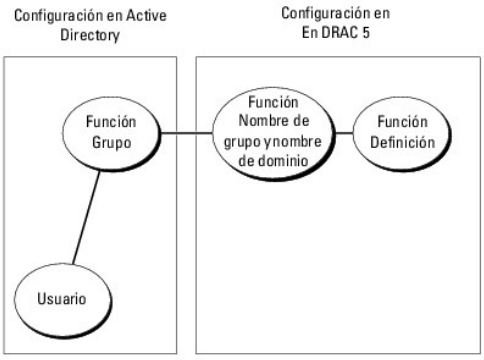


Tabla 6-1. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel predeterminado de privilegios	Permisos concedidos	Máscara de bits
Grupo de funciones 1	Administrador	Iniciar sesión en el DRAC, Configurar el DRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la redirección de consola, Acceder a medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000001ff
Grupo de funciones 2	Usuario avanzado	Iniciar sesión en el DRAC, Borrar registros, Ejecutar comandos de control de servidor, Acceder a la redirección de consola, Acceder a los medios virtuales, Probar alertas	0x000000f9
Grupo de funciones 3	Usuario invitado	Iniciar sesión en el DRAC	0x00000001
Grupo de funciones 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de funciones 5	Ninguno	Sin permisos asignados	0x00000000

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

Hay dos maneras de activar el esquema estándar de Active Directory:

- Con la interfaz web de usuario del DRAC 5. Consulte "Configuración del DRAC 5 con el esquema estándar de Active Directory y la interfaz basada en web".
- Con la herramienta de CLI de RACADM. Consulte "Configuración del DRAC 5 con el esquema estándar de Active Directory y RACADM".

Configuración del esquema estándar de Active Directory para acceder al DRAC 5

Usted debe realizar los pasos siguientes para configurar Active Directory antes de que un usuario de Active Directory pueda acceder al DRAC 5:

1. En un servidor de Active Directory (controlador de dominio), abra el complemento de usuarios y equipos de Active Directory.
2. Cree un grupo o seleccione un grupo existente. El nombre del grupo y el nombre de este dominio deberá ser configurado en el DRAC 5 con la interfaz web o con RACADM (consulte "Configuración del DRAC 5 con el esquema estándar de Active Directory y la interfaz basada en web" o "Configuración del DRAC 5 con el esquema estándar de Active Directory y RACADM").
3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al DRAC 5.

Configuración del DRAC 5 con el esquema estándar de Active Directory y la interfaz basada en web

1. Abra una ventana del explorador web compatible.
2. Inicie sesión en la interfaz basada en web de DRAC 5.
3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
4. Haga clic en la ficha **Configuración** y seleccione **Active Directory**.
5. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.
6. En la sección Configuración común:
   a. Seleccione la casilla de marcación **Activar Active Directory**.
   b. Escriba el **nombre del dominio raíz**. El **nombre del dominio raíz** es el nombre del dominio raíz completamente calificado para el bosque.
   c. Escriba el **Tiempo de espera** en segundos.
7. Haga clic en **Utilizar 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 un Grupo de funciones.

   Aparecerá la página Configurar grupo de funciones, que incluye el Nombre de grupo, Dominio de grupo y Privilegios del grupo de funciones del grupo de funciones.
10. Escriba el **Nombre de grupo**. El nombre de grupo identifica el grupo de funciones en el Active Directory asociado con la tarjeta DRAC 5.
11. Escriba el **Dominio de grupo**. El **Nombre de grupo** es el nombre completo del dominio raíz para el bosque.
12. En la página Privilegios del grupo de funciones, defina los privilegios del grupo.

    La Tabla 6-12 describe los Privilegios del grupo de funciones.

    La Tabla 6-13 describe los Permisos del grupo de funciones. Si modifica alguno de los permisos, el Privilegio del grupo de funciones ya 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 de CA de raíz del bosque de dominio en el DRAC 5.
    a. Seleccione la casilla de marcación **Cargar certificado de CA de Active Directory** y después haga clic en **Siguiente**.
    b. En la página **Carga del certificado**, escriba la ruta de acceso del archivo del certificado o desplácese al directorio del archivo del certificado.

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

    Los certificados SSL de los controladores de dominio deberán haber sido firmados por la CA raíz. Compruebe que el certificado raíz de CA esté disponible en la estación de administración que tiene acceso al DRAC 5 (consulte "Exportación del certificado de CA raíz del controlador de dominio al DRAC 5").
    c. Haga clic en Aplicar.

    El servidor web de DRAC 5 se reinicia automáticamente después de hacer clic en **Aplicar**.
17. Cierre la sesión y vuelva a iniciar sesión en DRAC 5 para completar la configuración de las funciones de Active Directory para DRAC 5.
18. En el árbol **Sistema**, haga clic en **Acceso remoto**.
19. Haga clic en la ficha Configuración y después haga clic en Red.

    Aparecerá la página **Configuración de la red**.
20. Si **Usar DHCP (para la dirección IP del NIC)** está seleccionado en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

Para introducir manualmente una dirección IP del servidor DNS, deseleccione **Usar DHCP para obtener las direcciones del servidor DNS** y escriba las direcciones IP principal y alternativa del servidor DNS.

21. Haga clic en **Aplicar cambios**.

La configuración de la función de esquema estándar de Active Directory del DRAC 5 ha concluido.

Configuración del DRAC 5 con el esquema estándar de Active Directory y RACADM

Use los siguientes comandos para configurar la función de Active Directory del DRAC 5 con esquema estándar por medio de la CLI de RACADM en lugar de la interfaz basada en web.

1. Abra una petición de comando y escriba los siguientes comandos de racadm:

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

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre completo del dominio raíz>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupName <nombre común del grupo de funciones>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupDomain <nombre completo de dominio>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupPrivilege <número de la máscara de bits para los permisos del usuario específico>

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

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

NOTA: Para obtener los valores del número de máscara de bits, consulte Tabla B-4.

2. Si DHCP está activado en el DRAC 5 y desea usar el DNS proporcionado por el servidor DHCP, escriba los siguientes comandos:

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

3. Si DHCP está desactivado en el DRAC 5, o si usted desea introducir manualmente la dirección IP de DNS, escriba los siguientes comandos:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

Generalidades del esquema ampliado de Active Directory

Hay dos maneras de activar el esquema ampliado de Active Directory:

- Con la interfaz web de usuario del DRAC 5. Consulte "Configuración del DRAC 5 con el esquema ampliado de Active Directory y la interfaz basada en web".
- Con la herramienta de CLI de RACADM. Consulte "Configuración del DRAC 5 con el esquema ampliado de Active Directory y RACADM".

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden ampliar la base de datos de Active Directory al agregar sus propios atributos y clases únicos para solucionar necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que es se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de Identificadores de Objeto de Active Directory (OID) de modo que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para ampliar el esquema en Active Directory, Dell recibió OID únicos, extensiones de nombre únicas e identificaciones de atributo vinculadas exclusivamente para nuestros atributos y clases, los cuales se agregan al servicio de directorio.

La extensión de Dell es: dell

El OID base de Dell es: 1.2.840.113556.1.8000.1280

El rango del LinkID de RAC es: 12070 a 12079

La base de datos de OID de Active Directory que mantiene Microsoft puede consultarse en http://msdn.microsoft.com/certification/ADAcctInfo.asp, al introducir nuestra extensión Dell.

Descripción de las extensiones de esquema de RAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha ampliado el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos de RAC. Este modelo proporciona al administrador la máxima flexibilidad sobre las combinaciones diferentes de usuarios, privilegios de RAC y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción general de los objetos de Active Directory

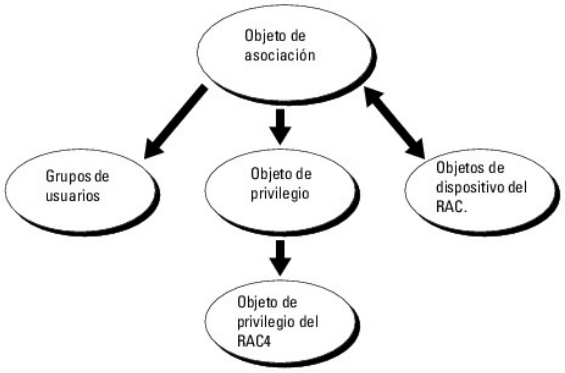
Para cada uno de los RAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de RAC. Puede crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios,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

Sin embargo, cada objeto de asociación puede ser vinculado (o, puede unir usuarios, grupos de usuarios u objetos de dispositivo de RAC) a sólo un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los RAC específicos.

El objeto del dispositivo del RAC es el eslabón al firmware de RAC para consultar a Active Directory para la autentificación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autentificación y la autorización con Active Directory. Además, el administrador también debe agregar el sistema a por lo menos un objeto de asociación para que los usuarios se puedan autenticar.

La Figura 6-2 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

Figura 6-2. Configuración típica de los objetos de Active Directory



NOTA: El objeto de privilegio del RAC se aplica al DRAC 4 y al DRAC 5.

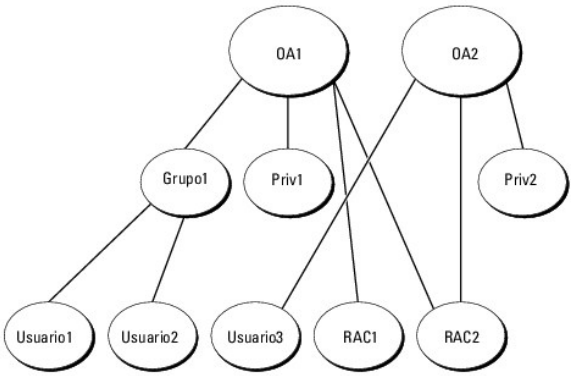
Usted puede crear tantos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de RAC para cada RAC (DRAC 5) en la red que desea integrar con Active Directory para la autenticación y autorización con el RAC (DRAC 5).

El objeto de asociación permite esta cantidad de usuarios y/o grupos así como objetos de dispositivo de RAC. Sin embargo, el objeto de asociación sólo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los usuarios que tienen privilegios en los RAC (DRAC 5).

Además, se pueden configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, se tienen dos tarjetas DRAC 5 (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). Se quieren otorgar privilegios de administrador al usuario1 y al usuario2 en las dos tarjetas DRAC 5 y se desea dar un privilegio de inicio de sesión al usuario3 en la tarjeta RAC2. Figura 6-3 muestra cómo configurar los objetos de Active Directory en este caso.

Cuando se agregan grupos universales a partir de dominios independientes, se debe crear un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados creados por la utilidad Dell Schema Extender, son grupos locales de dominio y no funcionarán con grupos universales de otros dominios.

Figura 6-3. Configuración de objetos de Active Directory en un solo dominio



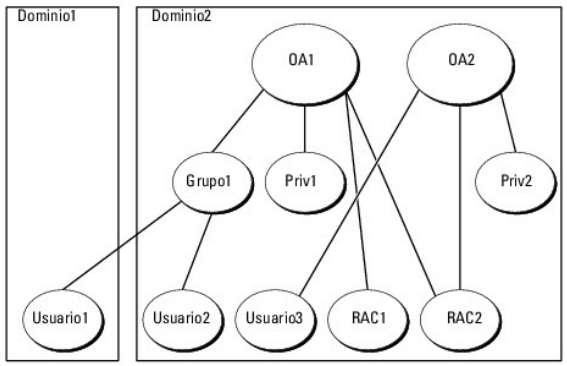
Para configurar los objetos en el caso de un solo dominio, realice las siguientes tareas:

1. Cree dos objetos de asociación.
2. Cree dos objetos de producto de RAC —RAC1 y RAC2— que representen las dos tarjetas DRAC 5.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
4. Agrupe al usuario1 y usuario2 en el Grupo1.
5. Agregue el Grupo1 como miembro en el objeto de asociación 1 (OA1), Priv1 como objeto de privilegio en OA1, y RAC1 y RAC2 como dispositivos de RAC en OA1.
6. Agregue el usuario3 como miembro en el objeto de asociación 2 (OA2), Priv2 como objeto de privilegio en OA2, y RAC2 como dispositivo de RAC en OA2.

Consulte "Cómo agregar usuarios y privilegios de DRAC 5 a Active Directory" para obtener instrucciones detalladas.

La Figura 6-4 muestra un ejemplo de los objetos de Active Directory en varios dominios. En este escenario, se tienen dos tarjetas DRAC 5 (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). El usuario1 está en el Dominio1; el usuario2 y el usuario 3 están en el Dominio2. En este escenario, configure el usuario1 y el usuario2 con privilegios de administrador en ambas tarjetas DRAC 5 y configure el usuario 3 con privilegios de inicio de sesión en la tarjeta RAC2.

Figura 6-4. Configuración de objetos de Active Directory en múltiples dominios



Para configurar los objetos en el caso de varios dominios, realice las siguientes tareas:

1. Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2. Cree dos objetos de asociación, OA1 (con ámbito universal) y OA2, en cualquier dominio.

   La Figura 6-4 muestra los objetos en el Dominio2.
3. Cree dos objetos de producto de RAC —RAC1 y RAC2— que representen las dos tarjetas DRAC 5.
4. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
5. Agrupe al usuario1 y usuario2 en el Grupo1. El ámbito de grupo del Grupo1 debe ser Universal.
6. Agregue el Grupo1 como miembro en el objeto de asociación 1 (OA1), Priv1 como objeto de privilegio en OA1, y RAC1 y RAC2 como dispositivos de RAC en OA1.
7. Agregue el usuario3 como miembro en el objeto de asociación 2 (OA2), Priv2 como objeto de privilegio en OA2, y RAC2 como dispositivo de RAC en OA2.

Configuración del esquema ampliado de Active Directory para acceder al DRAC 5

Antes de que pueda usar Active Directory para tener acceso al DRAC 5, configure el software de Active Directory y el DRAC 5 con los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (consulte "Extensión del esquema de Active Directory").
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory").
3. Agregue usuarios del DRAC 5 y los privilegios a Active Directory (consulte "Cómo agregar usuarios y privilegios de DRAC 5 a Active Directory").
4. Active SSL en cada uno de los controladores de dominio (consulte "Activación de SSL en un controlador de dominio").
5. Configure las propiedades de Active Directory del DRAC 5 por medio de la interfaz basada en web del DRAC 5 o mediante RACADM (consulte "Configuración del DRAC 5 con el esquema ampliado de Active Directory y la interfaz basada en web" o "Configuración del DRAC 5 con el esquema ampliado de Active Directory y RACADM").

Extensión del esquema de Active Directory

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

Puede ampliar el esquema por medio de uno de los métodos siguientes:

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

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation*, en los siguientes directorios respectivamente:

- Unidad de DVD**:\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- Unidad de DVD**:\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender**

Para usar los archivos LDIF, consulte las instrucciones en el archivo readme (léame) que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, consulte "Uso del ampliador de esquema de Dell".

Puede copiar y ejecutar el ampliador de esquema o los archivos LDIF desde cualquier ubicación.

Uso del ampliador de esquema de Dell

AVISO: Dell Schema Extender utiliza el archivo **SchemaExtenderOem.ini**. Para asegurar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
2. Lea y comprenda la advertencia y haga clic en Siguiente.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar el ampliador de esquema de Dell.
5. Haga clic en **Finish** (Finalizar).

El esquema ha sido extendido. Para verificar la ampliación del esquema, utilice la Consola de administración de Microsoft (MMC) y el complemento de esquema de Active Directory para verificar que existen los siguientes:

- Clases (consulte de la Tabla 6-2 a la Tabla 6-7)
- Atributos (Tabla 6-8)

Consulte la documentación de Microsoft para obtener más información sobre cómo activar y usar el complemento de esquema de Active Directory en el MMC.

Tabla 6-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 6-3. Clase dellRacDevice

OID	**1.2.840.113556.1.8000.1280.1.1.1.1**
Descripción	Representa el dispositivo RAC de Dell. El dispositivo RAC debe estar configurado como dellRacDevice en Active Directory. Esta configuración

	permite al DRAC 5 enviar consultas de LDAP (Protocolo de acceso de directorio ligero) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	**dellSchemaVersion** **dellRacType**

Tabla 6-4. Clase dellAssociationObject

OID	**1.2.840.113556.1.8000.1280.1.1.1.2**
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	**dellProductMembers** **dellPrivilegeMember**

Tabla 6-5. Clase dellRAC4Privileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Descripción	Esta clase se usa para definir los privilegios (derechos de autorización) del dispositivo DRAC 5.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabla 6-6. Clase dellPrivileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	**dellRAC4Privileges**

Tabla 6-7. Clas dellProduct

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

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

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

Lista de los objetos de dellPrivilege Dell que pertenecen a este atributo.	Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers Lista de los objetos dellRacDevices que pertenecen a esta función. Este atributo es el vínculo de avance al vínculo de retroceso dellAssociationMembers. Identificación del vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de redirección de consola en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comando de depuración en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Este atributo es el tipo de RAC actual para el objeto dellRacDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena en que se ignorar las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Lista de los miembros de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el eslabón de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Cuando amplía el esquema en Active Directory, debe ampliar también el complemento de usuarios y equipos de Active Directory de modo que el administrador pueda gestionar los dispositivos de RAC (DRAC 5), usuarios y grupos de usuarios, asociaciones de RAC y privilegios de RAC.

Cuando instala el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation*, puede ampliar el complemento si selecciona la opción **Extensión de Dell para el complemento de usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la Guía de instalación rápida del software Dell OpenManage para obtener más instrucciones sobre la instalación del software de administración de sistemas.

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

Instalación de Administrator Pack

Instale Administrator Pack en cada sistema que administre los objetos de DRAC 5 de Active Directory. Si no instala Administrator Pack, no podrá ver el objeto RAC de Dell en el contenedor.

Consulte "Cómo abrir el complemento de usuarios y equipos de Active Directory" para obtener más información.

Cómo abrir el complemento de usuarios y equipos de Active Directory

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

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

   Si no está conectado en el controlador de dominio, debe tener el Administrator Pack de Microsoft correspondiente instalado en el sistema local. Para instalar este Administrator Pack, haga clic en **Inicio**→ **Ejecutar**, escriba `MMC` y oprima **Entrar**.

   Aparecerá la ventana Consola de administración de Microsoft (MMC).
2. En la ventana **Consola 1**, haga clic en Archivo (o en Consola, en los sistemas que ejecutan Windows 2000).
3. Haga clic en **Agregar o quitar complemento**.
4. Seleccione el complemento Usuarios y equipos de Active Directory y haga clic en Agregar.
5. Haga clic en **Cerrar** y haga clic en **OK (Aceptar)**.

Cómo agregar usuarios y privilegios de DRAC 5 a Active Directory

El complemento de usuarios y equipos de Active Directory ampliado por Dell le permite agregar usuarios y privilegios de DRAC 5 al crear objetos de RAC, de asociación y de privilegio. Para agregar cada tipo de objeto, realice los pasos a continuación:

- Cree un objeto de dispositivo de RAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto de dispositivo de RAC

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

   Aparece la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del DRAC 5 que escribirá en el paso a de la sección "Configuración del DRAC 5 con el esquema ampliado de Active Directory y la interfaz basada en web".
4. Seleccione **Objeto de dispositivo de RAC**.
5. Haga clic en **OK (Aceptar)**.

Creación de un objeto de privilegio

NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

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

Aparece la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
7. Haga clic en la ficha **Privilegios de RAC** y seleccione los privilegios que desea el usuario tenga (para obtener más información, consulte Tabla 5-4).

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El ámbito de la asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Cuando cree un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objeto que quiere agregar.

Por ejemplo, si selecciona **Universal** los objetos de asociación sólo estarán disponibles cuando el dominio de Active Directory funcione en el modo nativo o superior.

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

Esto abrirá la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de asociación**.
5. Seleccione el ámbito para el **objeto de asociación**.
6. Haga clic en **OK (Aceptar)**.

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades de objeto de asociación**, puede asociar a usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta Windows 2000 o posteriores, utilice los grupos universales para abarcar dominios con los objetos de RAC o usuario.

Puede agregar a grupos de dispositivos de RAC y usuarios. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

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

Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentican en un dispositivo RAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

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

Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados con la red que están disponibles para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de RAC a un objeto de asociación.

Cómo agregar dispositivos de RAC o grupos de dispositivos de RAC

Para agregar dispositivos de RAC o grupos de dispositivos de RAC:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Escriba el nombre del dispositivo de RAC o del grupo de dispositivos de RAC y haga clic en **OK (Aceptar)**.
3. En la ventana Propiedades, haga clic en Aplicar y en **OK (Aceptar)**.

Configuración del DRAC 5 con el esquema ampliado de Active Directory y la interfaz basada en web

1. Abra una ventana del explorador web compatible.
2. Inicie sesión en la interfaz basada en web de DRAC 5.
3. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
4. Haga clic en la ficha **Configuración** y seleccione **Active Directory**.
5. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.
6. En la sección Configuración común:
   a. Seleccione la casilla de marcación **Activar Active Directory**.
   b. Escriba el **nombre del dominio raíz**. El **nombre del dominio raíz** es el nombre del dominio raíz completamente calificado para el bosque.
   c. Escriba el **Tiempo de espera** en segundos.
7. Haga clic en **Utilizar esquema ampliado** en la sección Selección del esquema de Active Directory.
8. En la sección Configuración del esquema ampliado:
   a. Escriba el **Nombre de DRAC**. Este nombre debe ser el mismo que el nombre común del nuevo objeto de RAC que creó en el controlador del dominio (consulte el paso 3 de Creación de un objeto de dispositivo de RAC).
   b. Escriba el **Nombre de dominio del DRAC** (por ejemplo, drac5.com). No use el nombre de NetBIOS. El **Nombre de dominio del DRAC** es el nombre completo de dominio del subdominio en donde se encuentra el objeto de dispositivo de RAC.
9. Haga clic en **Aplicar** para guardar la configuración de Active Directory.
10. Haga clic en **Volver al menú principal de Active Directory**.
11. Cargue el certificado de CA de raíz del bosque de dominio en el DRAC 5.
    a. Seleccione la casilla de marcación **Cargar certificado de CA de Active Directory** y después haga clic en **Siguiente**.
    b. En la página **Carga del certificado**, escriba la ruta de acceso del archivo del certificado o desplácese al directorio del archivo del certificado.

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

    Los certificados SSL de los controladores de dominio deberán haber sido firmados por la CA raíz. Tenga el certificado raíz de CA disponible en la estación de administración mientras accede al DRAC 5 (consulte "Exportación del certificado de CA raíz del controlador de dominio al DRAC 5").
    c. Haga clic en Aplicar.

    El servidor web de DRAC 5 se reinicia automáticamente después de hacer clic en **Aplicar**.
12. Cierre la sesión y vuelva a iniciar sesión en DRAC 5 para completar la configuración de las funciones de Active Directory para DRAC 5.
13. En el árbol **Sistema**, haga clic en **Acceso remoto**.
14. Haga clic en la ficha Configuración y después haga clic en Red.

    Aparecerá la página **Configuración de la red**.
15. Si **Usar DHCP (para la dirección IP del NIC)** está seleccionado en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

    Para introducir manualmente una dirección IP del servidor DNS, deseleccione **Usar DHCP para obtener las direcciones del servidor DNS** y escriba las direcciones IP principal y alternativa del servidor DNS.
16. Haga clic en **Aplicar cambios**.

La configuración de la función de esquema ampliado de Active Directory del DRAC 5 ha concluido.

Configuración del DRAC 5 con el esquema ampliado de Active Directory y RACADM

Use los siguientes comandos para configurar la función de Active Directory del DRAC 5 con esquema ampliado por medio de la herramienta de CLI de RACADM en lugar de la interfaz basada en web.

1. Abra una petición de comando y escriba los siguientes comandos de racadm:

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

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

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

```
racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre completo del dominio raíz>
```

```
racadm config -g cfgActiveDirectory -o cfgADRacName <nombre común del RAC>
```

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

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

2. Si desea especificar un servidor de catálogo global o LDAP, o un dominio de objeto de asociación en lugar de utilizar los servidores que ofrece el servidor DNS para buscar un nombre de usuario, escriba el siguiente comando para activar la opción **Especificar servidor**:

```
racadm config -g cfgActive Directory -o cfgADSpecifyServer Enable 1
```

NOTA: Si utiliza esta opción, el nombre de host en el certificado de CA no se comparará con el nombre del servidor especificado. Esto resulta particularmente útil si usted es administrador del DRAC porque permite introducir un nombre de host así como una dirección IP.

Después de activar la opción **Especificar servidor**, puede especificar un servidor LDAP o de catálogo global con una dirección IP o un nombre de dominio completo (FQDN) del servidor. El nombre completo de dominio consiste en el nombre de host y el nombre de dominio del servidor.

NOTA: Si utiliza la autenticación de Active Directory con Kerberos, indique sólo el nombre de dominio completo del servidor, ya que el sistema no le permitirá especificar una dirección IP. Para obtener más información, consulte "Activación de la autenticación con Kerberos".

Para especificar un servidor LDAP por medio de la interfaz de línea de comandos (CLI), escriba:

```
racadm config -g cfgActive Directory -o cfgADDomainController <nombre completo de dominio o dirección IP>
```

Para especificar un servidor de catálogo global por medio de la interfaz de línea de comandos (CLI), escriba:

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <nombre completo de dominio o dirección IP>
```

Para especificar un dominio de objeto de asociación por medio de la interfaz de línea de comandos (CLI), escriba:

```
racadm config -g cfgActive Directory -o cfgAODomain <dominio>:<nombre completo de dominio o dirección IP>
```

donde <dominio> indica el dominio en el que reside el objeto de asociación, en tanto IP/FQDN es la dirección IP o el nombre completo de dominio del host específico (controlador del dominio) con el que se conecta el DRAC 5.

Para especificar el objeto de asociación, asegúrese de proporcionar la dirección IP o nombre de dominio completo también del servidor de catálogo global.

NOTA: Si especifica la dirección IP como 0.0.0.0, el DRAC 5 no buscará ningún servidor.

Puede especificar una lista de servidores LDAP o de catálogo global u objetos de asociación separados por comas. El DRAC 5 permite especificar hasta cuatro direcciones IP o nombres de host.

Si el LDAPS no se configura correctamente para todos los dominios y aplicaciones, la activación del mismo puede producir resultados inesperados durante el funcionamiento de las aplicaciones o dominios existentes.

Si configura el controlador de dominio en la opción **Especificar servidor** del DRAC y el objeto de asociación contiene el objeto de RAC y usuario en el mismo dominio, el inicio de sesión de Active Directory por medio de Extended Schema se realizará con éxito. Sin embargo, si el objeto de RAC o de usuario del objeto de asociación proviene de un dominio diferente y sólo se proporciona la información del controlador de dominio, el inicio de sesión de Active Directory por medio de Extended Schema no podrá realizarse. En este caso, deberá configurar la opción de catálogo global para poder iniciar sesión.

3. Si DHCP está activado en el DRAC 5 y desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando:

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

4. Si DHCP está desactivado en el DRAC 5, o si usted desea introducir manualmente la dirección IP de DNS, escriba los siguientes comandos:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

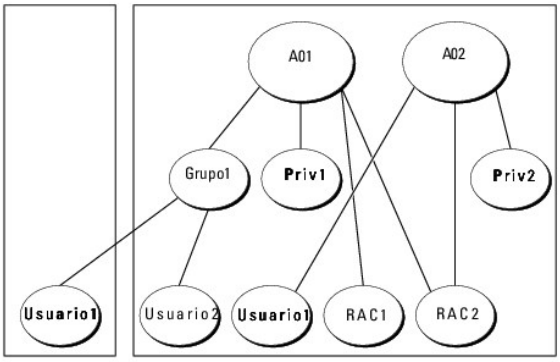
5. Haga clic en **Entrar** para completar la configuración de la función Active Directory de DRAC 5.

Acumulación de privilegios con el esquema ampliado

El mecanismo de autenticación del esquema ampliado admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados con el mismo usuario entre distintos objetos de asociación. En otras palabras, la autenticación del esquema ampliado acumula privilegios para permitir al usuario el súper conjunto de todos los privilegios asignados que corresponden a los distintos objetos de privilegio asociados al mismo usuario.

La Figura 6-5 muestra un ejemplo de la acumulación de privilegios por medio del esquema ampliado.

Figura 6-5. Acumulación de privilegios para un usuario



La figura muestra dos objetos de asociación: OA1 y OA2. Estos objetos de asociación pueden formar parte de los mismos dominios o de dominios distintos. El Usuario1 está asociado con el RAC1 y el RAC2 en ambos objetos de asociación. Por lo tanto, el Usuario1 ha acumulado privilegios que resultan de la combinación del conjunto de privilegios de los objetos Priv1 y Priv2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; y Priv2 tiene los privilegios: Inicio de sesión, Configurar el DRAC y Probar alertas. El Usuario1 tendrá ahora el conjunto de privilegios: Inicio de sesión, Medios virtuales, Borrar registros, Configurar el DRAC y Probar alertas, que es el conjunto de privilegios combinados de Priv1 y Priv2.

Así, la autenticación del esquema ampliado acumula privilegios para permitir que el usuario tenga el conjunto máximo posible de privilegios considerando los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

Configuración y administración de certificados de Active Directory

Para acceder al Menú principal de Active Directory:

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Active Directory**.

La Tabla 6-9 muestra una lista de las opciones de la página **Menú principal de Active Directory**.

Tabla 6-9. Opciones de la página de menú principal de Active Directory

Campo	Descripción
Configurar Active Directory	Configura el nombre del DRAC de Active Directory, el nombre de dominio RAÍZ, el nombre de dominio del DRAC, el tiempo de espera de autenticación de Active Directory, la selección del esquema de Active Directory y el grupo de funciones.
Cargar un certificado de CA de Active Directory	Carga un certificado de Active Directory en el DRAC.
Descarga un certificado de servidor de DRAC	El administrador de descargas de Windows permite descargar un certificado de servidor de DRAC en el sistema.
Ver un certificado de CA de Active Directory	Muestra el certificado de Active Directory que fue cargado en el DRAC.

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 y administración de Active Directory**, introduzca la configuración de Active Directory.

   La Tabla 6-10 describe los valores de la página **Configuración y administración de Active Directory**.
3. Haga clic en **Aplicar** para guardar la configuración.
4. Haga clic en el botón correspondiente de la página **Configuración de Active Directory** para continuar. Consulte el apartado Tabla 6-11.

5. Para configurar los grupos de funciones para el esquema estándar de Active Directory, haga clic en el grupo de funciones individual (1 a 5). Consulte el apartado Tabla 6-12 y el apartado Tabla 6-13.

NOTA: Para guardar la configuración de la página Configuración y administración de Active Directory, debe hacer clic en Aplicar antes de avanzar a la página Grupo de funciones personalizado.

Tabla 6-10. Configuración de la página Configuración y administración de Active Directory.

Valor	Descripción
Activar Active Directory	Activa Active Directory. Seleccionada=activado; deseleccionada=desactivado.
Nombre del dominio RAÍZ	El nombre de dominio RAÍZ de Active Directory. De manera predeterminada, este valor es **NULO**. El nombre debe ser un nombre válido de dominio que tenga *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios entre los caracteres y *y* es un tipo válido de dominio como com, edu, gov, int, mil, net, org.
Tiempo de espera	El tiempo en segundos de espera para que terminen las consultas a Active Directory. El valor mínimo es igual a 15 segundos o más. El valor predeterminado es 120 segundos.
Usar el esquema estándar	Utiliza el esquema estándar con Active Directory
Usar el esquema ampliado	Utiliza el esquema ampliado con Active Directory
Nombre del DRAC	El nombre que identifica de manera exclusiva la tarjeta DRAC 5 en Active Directory. De manera predeterminada, este valor es **NULO**. El nombre debe ser una cadena de 1 a 254 caracteres ASCII sin espacios entre los caracteres.
Nombre del dominio de DRAC	El nombre DNS (cadena) del dominio, en donde reside el objeto DRAC 5 de Active Directory. De manera predeterminada, este valor es **NULO**. El nombre debe ser un nombre válido de dominio que tenga *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios entre los caracteres y *y* es un tipo válido de dominio como com, edu, gov, int, mil, net, org.
Grupos de funciones	La lista de grupos de funciones asociada con la tarjeta DRAC 5. Para cambiar la configuración de un grupo de función, haga clic en el número del grupo de funciones, en la lista de grupos de funciones. Aparecerá la ventana Configurar grupo de funciones. **NOTA:** Si hace clic en el vínculo del grupo de funciones antes de aplicar la configuración de la página Configuración y administración de Active Directory, perderá la configuración.
Nombre de grupo	El nombre que identifica el grupo de funciones en el Active Directory asociado con la tarjeta DRAC 5.
Dominio de grupo	El dominio en donde se encuentra el grupo.
Privilegio de grupo	El nivel de privilegio del grupo.

Tabla 6-11. Botones de la página Configuración y administración de Active Directory

Botón	Descripción
Imprimir	Imprime la página **Configuración y administración de Active Directory**.
Aplicar	Guarda los cambios que se hicieron en la página **Configuración y administración de Active Directory**.
Volver al menú principal de Active Directory	Regresa a la página **Menú principal de Active Directory**.

Tabla 6-12. Privilegios del grupo de funciones

Valor	Descripción
Nivel de privilegio del grupo de funciones	Especifica el privilegio máximo del usuario del DRAC como uno de los siguientes: Administrador, Usuario avanzado, Usuario invitado, Ninguno o Personalizado. Consulte la Tabla 6-13 para ver los permisos del **Grupo de funciones**
Iniciar sesión en el DRAC	Activa el inicio de sesión del usuario en el DRAC.
Configurar el DRAC	Activa la capacidad de configuración para el usuario del DRAC.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Borrar registros	Activa la capacidad del usuario de borrar los registros del DRAC.
Ejecutar comandos de control del servidor	Activa la capacidad del usuario de ejecutar comandos de racadm.
Acceder a redirección de consola	Activa la capacidad del usuario de ejecutar redirección de consola.
Acceder a los medios virtuales	Activa la capacidad del usuario de ejecutar y usar los medios virtuales.
Probar alertas	Activa la capacidad del usuario de enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Activa la capacidad del usuario de ejecutar comandos de diagnóstico.

Tabla 6-13. Permisos del grupo de funciones

Propiedad	Descripción
Administrador	Iniciar sesión en el DRAC, Configurar el DRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la redirección de consola, Acceder a medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
Usuario avanzado	Iniciar sesión en el DRAC, Borrar registros, Ejecutar comandos de control de servidor, Acceder a la redirección de consola, Acceder a los medios virtuales, Probar alertas
Usuario invitado	Iniciar sesión en el DRAC
Personalizado	Selecciona cualquier combinación de los siguientes permisos: Iniciar sesión en el DRAC, Configurar el DRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de acciones de 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 de un certificado**, en el campo **Ruta de acceso del archivo**, escriba la ruta de acceso del archivo del certificado o haga clic en **Examinar** para navegar al archivo de certificado.

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

3. Haga clic en **Aplicar**.
4. Haga clic en el botón correspondiente de la página **Carga de un certificado** para continuar. Consulte el apartado Tabla 6-11.

Cómo descargar un certificado de servidor del DRAC

1. En la página **Menú principal de Active Directory**, seleccione **Descargar certificado de servidor de DRAC** y haga clic en **Siguiente**.
2. En la ventana **Descarga de archivo**, haga clic en **Guardar** y 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

Utilice la página **Menú principal de Active Directory** para ver el certificado de servidor de CA del DRAC 5.

1. En la página **Menú principal de Active Directory**, seleccione **Ver certificado de CA de Active Directory** y haga clic en **Siguiente**.

   La Tabla 6-14 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Haga clic en el botón correspondiente de la página **Ver certificado de CA de Active Directory** para continuar. Consulte el apartado Tabla 6-11.

Tabla 6-14. Información del certificado de CA de Active Directory

Campo	Descripción
Número de serie	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.
Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Activación de SSL en un controlador de dominio

Cuando el DRAC 5 autentica usuarios con un controlador de dominio de Active Directory, inicia una sesión de SSL con el controlador de dominio. En este momento, el controlador de dominio debe publicar un certificado firmado por la autoridad de certificación (CA); el certificado raíz que también se carga en el DRAC 5. En otras palabras, para que el DRAC 5 pueda autenticarse en *cualquier* controlador de dominio —sin importar si es el controlador de dominio raíz o

secundario— el controlador de dominio debe tener un certificado habilitado con SSL firmado por la CA del dominio.

Si va a usar la Entidad emisora de certificados raíz de Microsoft para asignar *automáticamente* todos los controladores de dominio a un certificado SSL, realice los pasos siguientes para activar el SSL en cada controlador de dominio:

1. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Política de seguridad del dominio**.
   b. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   c. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado de CA raíz del controlador de dominio al DRAC 5

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

1. Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **Start (Inicio)**→ **Run** (Ejecutar).
3. En el campo **Ejecutar**, escriba `mmc` y haga clic en **OK (Aceptar)**.
4. En la ventana **Consola 1** (MMC), haga clic en **Archivo (**o en **Consola** en sistemas con Windows 2000**)** y seleccione **Agregar o quitar complemento**.
5. En la ventana **Agregar o quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione la cuenta **Equipo** y haga clic en **Siguiente**.
8. Seleccione **Equipo local** y haga clic en **Terminar**.
9. Haga clic en **OK (Aceptar)**.
10. En la ventana **Consola 1**, amplíe la carpeta **Certificados**, amplíe la carpeta **Personal** y haga clic en la carpeta **Certificados**.
11. Localice el certificado de CA raíz y haga clic con el botón derecho en el mismo, seleccione **Todas las tareas** y haga clic en **Exportar...**
12. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
15. Cargue el certificado que guardó en el paso 14 en el DRAC 5.

Para cargar el certificado por medio de RACADM, consulte "Configuración del DRAC 5 con el esquema ampliado de Active Directory y la interfaz basada en web".

Para cargar el certificado por medio de la interfaz basada en web, realice el procedimiento a continuación:

a. Abra una ventana del explorador web compatible.
b. Inicie sesión en la interfaz basada en web de DRAC 5.
c. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
d. Haga clic en la ficha **Configuración** y después haga clic en **Seguridad**.
e. En la página **Menú principal de certificado de seguridad**, seleccione **Cargar certificado de servidor** y haga clic en **Aplicar**.
f. En la pantalla **Carga de un certificado**, realice uno de los pasos siguientes:
   - Haga clic en **Examinar** y seleccione el certificado.
   - En el campo Valor, escriba la ruta de acceso del certificado.
g. Haga clic en **Aplicar**.

Importación del certificado SSL del firmware del DRAC 5

NOTA: Si el servidor de Active Directory esta configurado para autenticar el cliente durante una fase de inicialización de sesión SSL, usted deberá cargar también el certificado de servidor del DRAC 5 en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de cliente durante la fase de inicialización de una sesión SSL.

Utilice el siguiente procedimiento para importar el certificado SSL del firmware del DRAC 5 a todas las listas de certificados confiables del controlador de dominio.

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

NOTA: Si el certificado SSL de firmware del DRAC 5 está firmado por una CA reconocida, no tiene que realizar los pasos descritos en esta sección.

El certificado SSL del DRAC 5 es idéntico al que se usa para el servidor web del DRAC 5. Todos los controladores DRAC 5 se envían con un certificado autofirmado predeterminado.

Para acceder al certificado por medio la interfaz basada en web del DRAC 5, seleccione **Configuración→ Active Directory→ Descargar el certificado de servidor de DRAC 5**.

1. En el controlador del dominio, abra una ventana **Consola de MMC** y seleccione **Certificados → Autoridades de certificación de raíz confiables**.
2. Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
3. Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.
4. Instale el certificado SSL del RAC en la **Autoridad de certificación de raíz confiable** de cada controlador de dominio.

   Si ha instalado su propio certificado, asegúrese que la CA que firma su certificado esté en la lista **Autoridad de certificación de raíz confiable**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.
5. Haga clic en **Siguiente** y seleccione si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o desplácese a un almacén de su elección.
6. Haga clic en **Terminar** y luego en **OK (Aceptar)**.

Cómo establecer la hora de SSL en el DRAC 5

Cuando el DRAC 5 autentica un usuario de Active Directory, el DRAC 5 también verifica el certificado publicado por el servidor de Active Directory para garantizar que el DRAC se comunica con un servidor de Active Directory autorizado.

Esta verificación también garantiza que la validez del certificado esté dentro del periodo que especifica el DRAC 5. Sin embargo, podría existir una incorrespondencia entre los husos horarios que se especifican en el certificado y el DRAC 5. Esto puede ocurrir cuando la hora del DRAC 5 refleja la hora del sistema local y el certificado refleja la hora con respecto al GMT.

Para garantizar que el DRAC 5 utilice la hora GMT para compararla con el periodo de vigencia del certificado, usted debe establecer el objeto de compensación de huso horario.

```
racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <valor de compensación>
```

Para obtener más información, consulte "cfgRacTuneTimezoneOffset (lectura/escritura)".

Configuración compatible de Active Directory

El algoritmo de consulta de Active Directory del DRAC 5 admite varios árboles en un solo bosque.

La autenticación de Active Directory del DRAC 5 admite el modo mixto (es decir, los controladores de dominio en el bosque ejecutan sistemas operativos diferentes, como Microsoft Windows NT® 4.0, Windows 2000 o Windows Server 2003). Sin embargo, todos los objetos utilizados por el proceso de consulta del DRAC 5 (entre usuario, objeto de dispositivo de RAC y objeto de asociación) deben estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory extendido para Dell verifica el modo y limita a los usuarios a fin de crear objetos a través de dominios si se encuentra en modo mixto.

Active Directory de DRAC 5 admite varios entornos de dominio siempre y cuando el nivel de la función de bosque de dominio se encuentre en el modo nativo o en el modo Windows 2003. Además, los grupos entre objeto de asociación, objetos de usuario de RAC, y objetos de dispositivo de RAC (incluso el objeto de asociación) deben ser grupos universales.

NOTA: El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory ampliado por Dell le obliga a crear estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes.

Uso de Active Directory para iniciar sesión en el DRAC 5

Puede utilizar Active Directory para iniciar sesión en DRAC 5 usando uno de los métodos siguientes:

- Interfaz basada en web
- RACADM remota
- Consola serie o Telnet.

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

<nombre_de_usuario@dominio>

O bien:

*<dominio>**<nombre_de_usuario>* o *<dominio>/<nombre_de_usuario>*

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

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

NOTA: No se pueden especificar nombres de dominio NetBIOS, como "América", porque estos nombres no se pueden resolver.

También puede iniciar en el DRAC 5 por medio de la tarjeta inteligente. Para obtener más información, consulte "Inicio de sesión en el DRAC 5 mediante la autenticación con tarjeta inteligente de Active Directory".

Uso del inicio de sesión único de Active Directory

Puede activar el DRAC 5 para utilizar Kerberos (un protocolo de autenticación de red) y permitir el inicio de sesión único en el DRAC 5. Para obtener más información sobre cómo configurar el DRAC 5 para usar esta función, consulte "Activación de la autenticación con Kerberos".

Configuración del DRAC 5 para usar el inicio de sesión único

1. Acceda a **Acceso remoto**→ ficha **Configuración** → subficha **Active Directory** → y seleccione **Configurar Active Directory**.
2. En la página **Configuración y administración de Active Directory**, seleccione **Inicio de sesión único**.

Esta opción le permite iniciar sesión en el DRAC 5 directamente después de conectarse con la estación de trabajo.

Conexión con el DRAC 5 mediante inicio de sesión único

1. Inicie sesión en su estación de trabajo por medio de su cuenta de red.
2. Acceda a la página Web del DRAC por medio del protocolo https.

https://*<dirección IP>*

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

https://<*dirección IP*>:<*número de puerto*>

donde <*dirección IP*> es la dirección IP del DRAC 5 y *número de puerto* corresponde al número de puerto HTTPS.

Aparecerá la página Inicio de sesión único del DRAC 5.

3. Haga clic en **Iniciar sesión**.

El DRAC 5 iniciará su sesión por medio de las credenciales que fueron capturadas en el sistema operativo cuando inició sesión mediante una cuenta válida de Active Directory.

Preguntas más frecuentes

¿Hay alguna restricción para la configuración del controlador de dominio de SSL?

Sí Los certificados SSL de todos los servidores de Active Directory en el bosque deben ser firmados por la misma CA raíz ya que el DRAC 5 sólo permite cargar un certificado SSL de CA confiable.

Creé y cargué un nuevo certificado de RAC y ahora la interfaz basada en web no se ejecuta.

Si usa servicios de Certificate Server de Microsoft para generar el certificado de RAC, una causa posible de esto es que haya elegido por descuido **Certificado de usuario** en vez de **Certificado de web** al crear el certificado.

Para recuperarse, genere una CSR y después cree un nuevo certificado de web a partir de los servicios Certificate Server de Microsoft y cárguelo por medio de la CLI de RACADM desde el sistema administrado con los siguientes comandos de racadm:

```
racadm sslcsrgen [-g] [-u] [-f {nombre_de_archivo}]

racadm sslcertupload -t 1 -f {cert_SSL_de_web}
```

¿Qué puedo hacer si no puedo iniciar sesión en el DRAC 5 usando la autenticación de Active Directory? ¿Cómo soluciono el problema?

1. Asegúrese de usar el nombre de dominio de usuario correcto durante un inicio de sesión y no el nombre de NetBIOS.
2. Si tiene una cuenta de usuario de DRAC local, inicie sesión en el DRAC 5 con sus credenciales locales.

Después de haber iniciado sesión:

a. Compruebe que la casilla **Activar Active Directory** esté seleccionada en la página de configuración de Active Directory de DRAC 5.
b. Asegúrese que la configuración DNS sea correcta en la página de configuración de red del DRAC 5.
c. Compruebe que cargó el certificado de Active Directory de la CA raíz de Active Directory al DRAC 5.
d. Revise los certificados de SSL de controlador de dominio para asegurarse que no hayan expirado.
e. Asegúrese que **Nombre del DRAC**, **Nombre del dominio raíz** y **Nombre del dominio de DRAC** coincidan con la configuración de entorno de Active Directory.
f. Compruebe que la contraseña del DRAC 5 tiene un máximo de 127 caracteres. Aunque el DRAC 5 admite contraseñas de hasta 256 caracteres, Active Directory sólo admite contraseñas que tengan un máximo de 127 caracteres.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la autenticación de tarjeta inteligente

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Las versiones 1.30 y posteriores de Dell™ Remote Access Controller 5 (DRAC 5) con compatibles con la *autenticación de dos factores* para iniciar sesión en la interfaz web del DRAC 5. Esta compatibilidad proviene de la función **Inicio de sesión de tarjeta inteligente** del DRAC 5.

Los esquemas tradicionales de autenticación usan nombres de usuario y contraseñas para autenticar a los usuarios. Esto proporciona una seguridad mínima.

Por el contrario, la autenticación de dos factores proporciona un nivel de seguridad más alto gracias a que requiere que los usuarios tengan una contraseña o PIN y una clave privada para un certificado digital.

La autenticación de dos factores requiere que los usuarios verifiquen su identidad al proporcionar *ambos* factores.

Configuración del inicio de sesión de tarjeta inteligente en el DRAC 5

Activa la función de inicio de sesión de tarjeta inteligente en el DRAC 5 a partir del menú **Acceso remoto**→ **Configuración**→ **Tarjeta inteligente**.

Si usted:

- **Desactiva** la configuración de la tarjeta inteligente, el sistema le solicitará un nombre de usuario y contraseña de conexión local o de Microsoft® Active Directory®.
- **Activa** o **Activa con racadm remota**, se le pedirán datos de inicio de sesión de tarjeta inteligente en los intentos de inicio de sesión subsiguientes a través de la interfaz gráfica de usuario.

  Cuando seleccione **Activar**, se desactivarán todas las interfaces fuera de banda de CLI (interfaz de línea de comandos), como Telnet, SSH, serie, racadm remota e IPMI mediante LAN. Esto se debe a que estos servicios sólo admiten la autenticación de un solo factor.

  Cuando seleccione **Activar con racadm remota**, se desactivarán todas las interfaces fuera de banda de CLI, salvo racadm remota.

  NOTA: Dell recomienda que el administrador de DRAC 5 utilice la opción **Activar con racadm remota** únicamente para acceder a la interfaz de usuario del DRAC 5 a fin de ejecutar secuencias de comandos por medio de los comandos de racadm remota. Si el administrador no necesita usar racadm remota, Dell recomienda que se utilice la opción **Activar** para el inicio de sesión de tarjeta inteligente. Asimismo, compruebe que la configuración de usuario local del DRAC 5 y/ o la configuración de Active Directory estén completas antes de activar el **Inicio de sesión de tarjeta inteligente**.

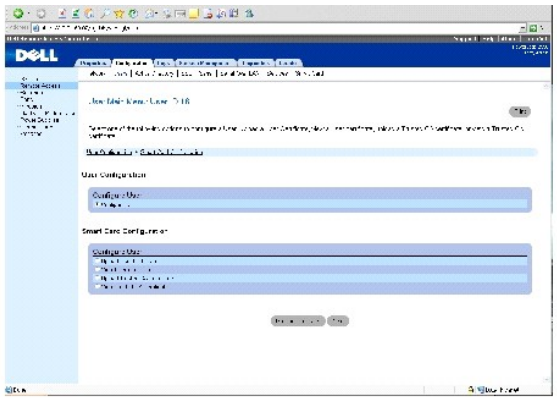
- **Activar comprobación de CRL para el inicio de sesión de tarjeta inteligente**, el certificado de DRAC del usuario, que se descarga del servidor de distribución de la Lista de revocación de certificado (CRL) se revisa en la CRL para determinar si se ha revocado.

  NOTA: Los servidores de distribución de CRL aparecen en los certificados de tarjeta inteligente de los usuarios.

Configuración de usuarios de DRAC 5 locales para inicio de sesión de tarjeta inteligente

Usted puede configurar usuarios de DRAC 5 locales para que puedan iniciar sesión en el DRAC 5 con la tarjeta inteligente. Diríjase a **Acceso remoto**→ **Configuración**→ **Usuarios**.

Figura 7-1. Página de administración de usuarios para tarjeta inteligente



Sin embargo, antes de que el usuario pueda iniciar sesión en el DRAC 5 con la tarjeta inteligente, usted debe cargar el certificado de tarjeta inteligente del usuario y el certificado de la CA (autoridad de certificados) de confianza para certificar el DRAC 5.

Exportación del certificado de tarjeta inteligente

Puede obtener el certificado del usuario mediante la exportación del certificado de tarjeta inteligente por medio del software de administración de tarjetas (CMS), de la tarjeta inteligente a un archivo en el formato codificado Base64. Habitualmente, el CMS puede obtenerse del proveedor de la tarjeta inteligente. Este archivo codificado se debe cargar como certificado del usuario en el DRAC 5. La autoridad de certificados de confianza que emite los certificados de usuario de tarjeta inteligente también deberá exportar el certificado de CA a un archivo en formato codificado Base 64. Usted debe cargar este archivo como certificado de CA de confianza del usuario. Configure el usuario con un nombre de usuario que forme el nombre de principio de usuario (UPN) del usuario en el certificado de la tarjeta inteligente.

NOTA: Para iniciar sesión en el DRAC 5, el nombre de usuario que configuró en el DRAC 5 debe ser exactamente igual que el Nombre principal de usuario (UPN) que figura en el certificado de tarjeta inteligente.

Por ejemplo, en caso que se haya emitido el certificado de tarjeta inteligente para el usuario, "usuario_muestra@domino.com", el nombre de usuario deberá configurarse como "usuario_muestra".

Configuración de usuarios de Active Directory para inicio de sesión de tarjeta inteligente

Para configurar los usuarios de Active Directory para que inicien sesión en el DRAC 5 por medio de la tarjeta inteligente, el administrador del DRAC 5 deberá configurar el servidor DNS, cargar el certificado de CA de Active Directory en el DRAC 5 y activar el inicio de sesión de Active Directory. Consulte "Uso del DRAC 5 con Microsoft Active Directory" para obtener más información sobre cómo configurar usuarios de Active Directory.

Puede configurar Active Directory a partir del menú **Acceso remoto**→ **Configuración**→ **Active Directory**.

Configuración de la tarjeta inteligente

NOTA: Para modificar esta configuración, debe tener permiso para **Configurar el DRAC 5**.

1. Amplíe el árbol **Sistema** y haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Tarjeta inteligente**.

3. Configure los valores de inicio de sesión de tarjeta inteligente.

   La Tabla 7-1 contiene información sobre los valores de la página **Tarjeta inteligente**.

4. Haga clic en **Aplicar cambios**.

Tabla 7-1. Valores de la tarjeta inteligente

Valor	Descripción
Configurar inicio de sesión de tarjeta inteligente	• Desactivado: desactiva el inicio de sesión de tarjeta inteligente. Los inicios de sesión subsiguientes en la interfaz gráfica de usuario mostrarán la página normal de inicio de sesión. Todas las interfaces de línea de comandos fuera de banda, incluso Secure Shell (SSH), Telnet, serie y RACADM remota toman el valor predeterminado correspondiente. • Activado: activa el inicio de sesión de tarjeta inteligente. Después de aplicar los cambios, cierre sesión, inserte su tarjeta inteligente y después haga clic en **Iniciar sesión** para introducir el PIN de la tarjeta inteligente. La activación del inicio de sesión de tarjeta inteligente desactiva todas las interfaces fuera de banda de CLI, incluso SSH, Telnet, serie, RACADM remota e IPMI mediante LAN. • Activado con racadm remota: activa el inicio de sesión de tarjeta inteligente junto con RACADM remota. Todas las demás interfaces fuera de banda de CLI se desactivan. **NOTA:** El inicio de sesión de tarjeta inteligente requiere que se configuren usuarios locales del DRAC 5 con los certificados correspondientes. Si se utiliza el inicio de sesión de tarjeta inteligente para que un usuario de Microsoft Active Directory inicie sesión, usted deberá asegurarse de configurar el certificado de usuario de Active Directory para dicho usuario. Puede configurar el certificado de usuario en la página **Usuarios**→**Menú principal de usuario**.
Activar comprobación de CRL para el inicio de sesión de tarjeta inteligente	Esta comprobación está disponible únicamente para usuarios de inicio de sesión de Active Directory. Seleccione esta opción si desea que el DRAC 5 revise la lista de revocación de certificados (CRL) para ver si el certificado de tarjeta inteligente del usuario ha sido revocado. El usuario no podrá iniciar sesión si: • El certificado de usuario aparece revocado en el archivo de CRL. • El DRAC no se puede comunicar con el servidor de distribución de CRL. • El DRAC no puede descargar la CRL. **NOTA:** Usted debe configurar correctamente la dirección IP del servidor DNS en la página **Configuración**→ **Red** para que esta comprobación se realice correctamente

---

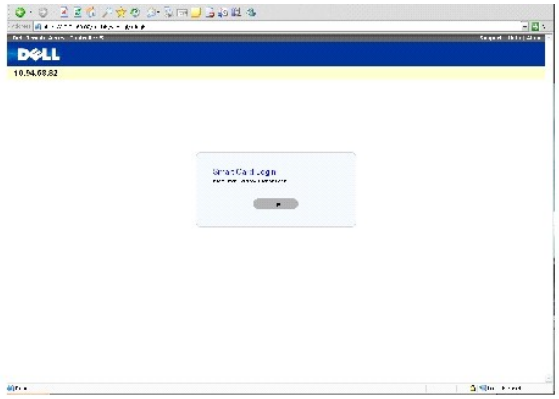
Inicio de sesión en el DRAC 5 por medio de la tarjeta inteligente

La interfaz web del DRAC 5 muestra la página de inicio de sesión de tarjeta inteligente de todos los usuario que fueron configurados para usar la tarjeta inteligente.

NOTA: Compruebe que la configuración de usuario local del DRAC 5 y/o la configuración de Active Directory esté completa antes de activar el inicio de sesión de tarjeta inteligente para el usuario.

NOTA: De acuerdo con la configuración del navegador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

Figura 7-2. Inicio de sesión en el DRAC 5 por medio de la tarjeta inteligente



1. Acceda a la página Web del DRAC 5 por medio del protocolo https.

https://<*dirección IP*>

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

https://<*dirección IP*>:<*número de puerto*>

donde <*dirección IP*> es la dirección IP del DRAC 5 y *número de puerto* corresponde al número de puerto HTTPS.

La página de inicio de sesión del DRAC 5 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente en el lector y haga clic en **Iniciar sesión**.

El DRAC 5 solicitará el PIN de la tarjeta inteligente.

3. Introduzca el PIN de la tarjeta inteligente y haga clic en **OK (Aceptar)**.

NOTA: Si usted es un usuario de Active Directory para quien se ha seleccionado la opción **Activar comprobación de CRL para inicio de sesión de tarjeta inteligente**, el DRAC 5 intentará descargar la CRL y buscará en ella el certificado del usuario. El inicio de sesión por medio de Active Directory fallará si el certificado aparece como revocado en la CRL o si la CRL no se puede descargar por cualquier motivo.

Ha iniciado sesión en el DRAC 5.

No obstante, si falla el inicio de sesión mediante la tarjeta inteligente y:

- ha activado el inicio de sesión de Active Directory para su cuenta de usuario, y
- es un usuario válido de Active Directory,
- debería haber configurado Active Directory para utilizar la autenticación mediante tarjeta inteligente (para obtener más información, consulte "Activación de la autenticación con Kerberos").

el DRAC 5 le permitirá iniciar sesión automáticamente.

Inicio de sesión en el DRAC 5 mediante la autenticación con tarjeta inteligente de Active Directory

1. Inicie sesión en el DRAC 5 por medio del protocolo https.

https://<*dirección IP*>

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

https://<*dirección IP*>:<*número de puerto*>

donde <*dirección IP*> es la dirección IP del DRAC 5 y *número de puerto* corresponde al número de puerto HTTPS.

La página de inicio de sesión del DRAC 5 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.

Se abrirá el cuadro de diálogo emergente para ingresar el PIN.

3. Introduzca el PIN y haga clic en **OK (Aceptar)**.

De esta forma habrá iniciado sesión en el DRAC 5 con sus credenciales, tal como están definidas en Active Directory.

Para obtener más información, consulte "Activación de la autenticación con Kerberos".

Solución de problemas de inicio de sesión de la tarjeta inteligente en el DRAC 5

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Compruebe que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows®. Windows admite una cantidad limitada de proveedores de servicios criptográficos (CSP) de tarjetas inteligentes.

Consejo: como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y revise si Windows detecta la tarjeta inteligente y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

No se puede iniciar sesión en el DRAC 5 local

Si un usuario de DRAC 5 local no puede iniciar sesión, revise si el nombre de usuario y los certificados de usuario que están cargados en el DRAC 5 han expirado. Los registros de rastreo del DRAC 5 pueden proporcionar mensajes importantes de registro relacionados con errores; sin embargo, los mensajes de error son, algunas veces, intencionalmente ambiguos por motivos de seguridad.

No se puede iniciar sesión en el DRAC 5 como usuario de Active Directory

Si no puede iniciar sesión en el DRAC 5 como usuario de Active Directory, trate de iniciar sesión en el DRAC 5 sin activar el inicio de sesión de tarjeta inteligente. Si ha activado la comprobación de CRL, intente iniciar sesión en Active Directory sin activar la comprobación de CRL. El registro de rastreo de DRAC 5 deberá proporcionar mensajes importantes si se presenta algún error de CRL.

También tiene la opción de desactivar el inicio de sesión de tarjeta inteligente a través de racadm local con el siguiente comando:

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

Regresar a la página de contenido

Regresar a la página de contenido

Activación de la autenticación con Kerberos

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Kerberos es un protocolo de autenticación de red que permite que los sistemas se comuniquen de forma segura a través de una red sin protección. Para ello, los sistemas deben demostrar su autenticidad.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® y Windows Server 2008 utilizan Kerberos como método de autenticación predeterminado.

A partir de la versión 1.40, el DRAC 5 utiliza Kerberos para dos tipos de mecanismos de autenticación: el inicio de sesión único y el inicio de sesión con tarjeta inteligente de Active Directory.

Para el inicio de sesión único, el DRAC 5 emplea las credenciales de usuario que fueron capturadas en el sistema operativo al iniciar sesión mediante una cuenta válida de Active Directory.

A partir de la versión 1.40 de DRAC 5, la autenticación de Active Directory utiliza el mecanismo de autenticación de dos factores (TFA) con tarjeta inteligente además de la combinación de nombre de usuario y contraseña como credenciales válidas.

Requisitos previos para el inicio de sesión único y la autenticación de Active Directory mediante tarjeta inteligente

- Configure el DRAC 5 para el inicio de sesión de Active Directory. Para obtener más información, consulte "Uso de Active Directory para iniciar sesión en el DRAC 5".
- Registre el DRAC 5 como computadora en el dominio raíz de Active Directory.
  a. Acceda a **Acceso remoto**→ ficha **Configuración** → subficha **Red** → **Configuración de red**.
  b. Indique una dirección IP de **servidor DNS estático/preferido** que sea válida. Este valor señala la dirección IP del servidor DNS que forma parte del dominio raíz, que autentica las cuentas de Active Directory de los usuarios.
  c. Seleccione **Registrar DRAC en DNS**.
  d. Brinde un **nombre de dominio DNS** válido.

  Consulte la *ayuda en línea del DRAC 5* para obtener información adicional.

Como el DRAC 5 es un dispositivo con un sistema operativo que no es Windows, ejecute la utilidad **ktpass** (que es parte de Microsoft® Windows®) en el controlador de dominio (servidor Active Directory) donde desea asignar el DRAC 5 a una cuenta de usuario de Active Directory. Por ejemplo,

```
C:\>ktpass -princ HOST/dracname.domain- name.com@domain-name.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -
out c:\krbkeytab
```

NOTA: El tipo de criptografía admitida por el DRAC 5 para la autenticación con Kerberos es DES-CBC-MD5.

Este procedimiento generará un archivo keytab que deberá cargar en el DRAC 5.

NOTA: Este archivo contiene una clave de cifrado y debe mantenerse guardado de manera segura.

Para obtener más información sobre la utilidad **ktpass**, visite el sitio Web de Microsoft:
http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

- La hora del DRAC 5 debe sincronizarse con el controlador de dominio de Active Directory.

Configuración del DRAC 5 para el inicio de sesión único y la autenticación de Active Directory mediante tarjeta inteligente

Cargue en el DRAC 5 el archivo keytab obtenido del dominio raíz de Active Directory:

1. Acceda a **Acceso remoto**→ ficha **Configuración** → subficha **Active Directory**.
2. Seleccione **Cargar Kerberos Keytab** y haga clic en **Siguiente**.
3. En la página **Carga de Kerberos Keytab**, acceda a la carpeta en la que guardó el archivo keytab y haga clic en **Cargar**.

Conexión con el DRAC 5 mediante inicio de sesión único

NOTA: Para conectarse con el DRAC 5, asegúrese de contar con los más recientes componentes de ejecución de las bibliotecas de Microsoft Visual C++ 2005. Para obtener más información, consulte el sitio Web de Microsoft.

1. Inicie sesión en el sistema por medio de una cuenta de Active Directory válida.
2. Escriba la dirección Web del DRAC 5 en la barra de direcciones del navegador.

   NOTA: De acuerdo con la configuración del navegador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para inicio de sesión único cuando utiliza esta función por primera vez.

   Ha iniciado sesión en el DRAC 5.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la redirección de consola con interfaz gráfica de usuario

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Esta sección contiene información sobre cómo usar la función de redirección de consola del DRAC 5.

Información general

La función de redirección de consola del DRAC 5 le permite tener acceso a la consola local de manera remota en modo gráfico o de texto. Con la redirección de consola, puede controlar uno o varios sistemas equipados con DRAC 5 desde un solo lugar.

Hoy, con el poder de conexión de redes y la Internet, usted no tiene que sentarse frente a cada servidor para realizar todo el mantenimiento de rutina. Puede administrar los servidores desde otra ciudad o hasta del otro lado del mundo desde una computadora de escritorio o 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 sistema administrado no indica que la consola ha sido redirigida.

La página **Redirección de consola** le permite administrar el sistema remoto usando el teclado, vídeo y mouse en la estación de administración local para controlar los dispositivos correspondientes en un sistema administrado remoto. Esta característica puede ser usada junto con la característica de medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- Sólo se admiten dos sesiones simultáneas de redirección de consola.
- Las sesiones de redirección de consola sólo pueden estar conectadas con un sistema remoto de destino.
- Usted no puede configurar una sesión de redirección de consola en el sistema local.
- Se requiere un ancho de banda disponible de red de 1 MB/s.

Velocidades de actualización y resoluciones de pantalla admitidas en el sistema administrado

La Tabla 9-1 muestra una lista de las resoluciones admitidas y las velocidades de actualización correspondientes para una sesión de redirección de consola que se ejecuta en el sistema administrado.

Tabla 9-1. Resoluciones de pantalla y velocidades de actualización admitidas

Resolución de pantalla	Velocidad de actualización (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1024 x 768	60, 70, 72, 75, 85
1280 x 1024	60

Configuración de la estación de administración

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

1. Instale y configure un explorador de web admitido. Consulte las siguientes secciones para obtener más información:
   - la *Matriz de compatibilidad de software de los sistemas Dell* en el sitio web de asistencia de Dell en **support.dell.com**.

     AVISO: La redirección de consola y los medios virtuales sólo admiten exploradores de web de 32 bits. El uso de exploradores de web de 64 bits puede producir resultados inesperados o la falla de las operaciones.

   - "Configuración de un explorador de web admitido"
2. Configure la resolución de la pantalla del monitor en al menos 1280 x 1024 píxeles a 60 Hz con 128 colores. De lo contrario, es posible que no vea la consola en **Modo de pantalla completa**.
3. Si utiliza el complemento Java para conectarse, asegúrese de que el sistema tenga instalado Java Virtual Machine (JVM) versión 1.4 o superior.

Configuración de la redirección de consola

1. En la estación de administración, abra un explorador de web admitido e inicie sesión en el DRAC 5. Consulte "Acceso a la interfaz basada en web" para obtener más información.
2. En el árbol **Sistema**, haga clic en **Sistema**.
3. Haga clic en la ficha **Consola** y después haga clic en **Configuración**.
4. En la página **Configuración de la redirección de consola**, utilice la información de la Tabla 9-2 para configurar la sesión de redirección de consola.
5. En las versiones 1.40 y posteriores del DRAC 5, existe la posibilidad de seleccionar el tipo de complemento **nativo** o **Java** que se desea instalar.

Haga clic en **Aplicar cambios**.

Tabla 9-2. Información de la página de configuración de la redirección de consola

Information	Descripción
Activado	Seleccionado = activado; deseleccionado = desactivado
N.° máx. de sesiones	Muestra el número máximo de redirecciones de consola que están disponibles.
Sesiones activas	Muestra el número de sesiones de redirección de consola activas.
Número del puerto de teclado y mouse	Predeterminado = 5900
Número del puerto de vídeo	Predeterminado = 5901
Cifrado de vídeo activado	Seleccionado = activado; deseleccionado = desactivado
Vídeo del servidor local activado	Seleccionado = activado; deseleccionado = desactivado
Tipo de complemento	Permite seleccionar el tipo de complemento **nativo** (ActiveX para Windows y XPI para Linux) o **Java**. **NOTA:** Si selecciona el complemento Java, asegúrese de que Java Virtual Machine (JVM) versión 1.4 o posterior ya esté instalado en el sistema.

Los botones que se muestran en la Tabla 9-3 están disponibles en la página **Configuración de la redirección de consola**.

Tabla 9-3. Botones de la página de configuración de la redirección de consola

Propiedad	Descripción
Imprimir	Imprime la página **Configuración de la redirección de consola**
Actualizar	Vuelve a cargar la página **Configuración de la redirección de consola**
Aplicar cambios	Guarda los valores de configuración.

NOTA: Con el DRAC 5 versión 1.30 y posteriores, usted puede desactivar la redirección de consola de un usuario remoto. Para obtener más información, consulte "Desactivación del KVM virtual remoto del DRAC 5".

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 visualizador. Al usar la aplicación Virtual KVM Viewer, puede controlar las funciones de mouse y teclado del sistema desde una estación de administración local o remota.

Para abrir una sesión de redirección de consola:

1. En la estación de administración, abra un explorador de web admitido e inicie sesión en el DRAC 5. Consulte "Acceso a la interfaz basada en web" para obtener más información.
2. En el árbol **Sistema**, haga clic en **Sistema** y después en la ficha **Consola**, haga clic en **Redirección de consola**.

NOTA: Si recibe una advertencia que le pide que instale y ejecute el complemento de redirección de consola, verifique la autenticidad del complemento y después haga clic en **Sí** para instalar y ejecutar el complemento. Si está ejecutando Firefox, reinicie el explorador y después vaya al paso 1.

3. En la página **Redirección de consola**, utilice la información de la Tabla 9-4 para verificar que haya una sesión de redirección de consola disponible.

Tabla 9-4. Información de la página de redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No
Cifrado de vídeo activado	Sí/No
Vídeo del servidor local activado	Sí/No
Estado	Conectado o desconectado
N.° máx. de sesiones	El número máximo de sesiones de redirección de consola admitidas
Sesiones activas	El número actual de sesiones de redirección de consola activas
Tipo de complemento	Indica el tipo de complemento seleccionado en la página **Configuración de la redirección de consola**.

Los botones en la Tabla 9-5 están disponibles en la página **Redirección de consola**.

Tabla 9-5. Botones de la página de redirección de consola

Botón	Definición
Actualizar	Actualiza la página **Configuración de la redirección de consola**
Conectar	Abre una sesión de redirección de consola en el sistema remoto de destino.
Imprimir	Imprime la página **Configuración de la redirección de consola**

4. Si hay una sesión de redirección de consola disponible, haga clic en **Conectar**.

Si el sistema se ejecuta en Linux y eligió instalar el complemento Java en la página **Configuración de la redirección de consola**, aparecerá un mensaje para que opte por **Abrir** o **Guardar** el archivo **.jnlp** en el sistema. Si decide guardar el archivo **.jnlp**, debe ejecutarlo de forma manual haciendo doble clic sobre el archivo guardado. Si descarga el archivo **.jnlp** sin ejecutarlo, el estado de Redirección de consola siempre aparecerá como **Conectando**.

Si el sistema se ejecuta en Windows y eligió instalar el complemento Java en la página **Configuración de la redirección de consola**, el sistema guardará el archivo **.jnlp** y lo ejecutará automáticamente.

NOTA: Si JVM no está instalado en el sistema, al hacer clic en **Conectar** el estado de Redirección de consola siempre aparecerá como **Conectando** hasta que haga clic en **Desconectar**.

NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

NOTA: Si una o varias ventanas de Alerta de seguridad aparecen en los pasos siguientes, lea la información en la ventana y haga clic en Sí para seguir.

La estación de administración se conecta al DRAC 5 y la pantalla de escritorio del sistema remoto aparece en la aplicación Dell Digital KVM Viewer.

5. Si aparecen dos apuntadores del mouse en el escritorio del sistema remoto, sincronice los apuntadores del mouse en la estación de administración y el sistema remoto. Consulte "Sincronización de los apuntadores del mouse".

Desactivación o activación del vídeo local

Para desactivar o activar el vídeo local, realice el siguiente procedimiento:

1. En la estación de administración, abra un explorador de web admitido e inicie sesión en el DRAC 5. Consulte "Acceso a la interfaz basada en web" para obtener más información.
2. En el árbol **Sistema**, haga clic en **Sistema**.
3. Haga clic en la ficha **Consola** y después haga clic en **Configuración**.
4. Si desea activar (encender) el vídeo local en el servidor, en la página **Configuración de la redirección de consola**, seleccione la casilla Vídeo del servidor local activado y después haga clic en Aplicar cambios. El valor predeterminado es encendido.
5. Si desea desactivar (apagar) el vídeo local en el servidor, en la página **Configuración de la redirección de consola**, deseleccione la casilla Vídeo del servidor local activado y después haga clic en Aplicar cambios.

La página Redirección de consola muestra el estado del vídeo del servidor local.

NOTA: La función de vídeo del servidor local activado se admite en todos los sistemas x9xx PowerEdge, excepto en los PowerEdge SC1435 y 6950.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, sólo se desactivará el monitor conectado al servidor local.

NOTA: Con el DRAC 5 versión 1.30 y posteriores, usted puede desactivar la redirección de consola de un usuario remoto. Para obtener más información, consulte "Desactivación del KVM virtual remoto del DRAC 5".

Uso de Video Viewer

Video Viewer tiene una interfaz de usuario entre la estación de administración y el sistema remoto, lo que permite ver la pantalla de escritorio del sistema remoto 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 ofrece varios ajustes de control como calibración de vídeo, aceleración de mouse e instantáneas. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Cuando se inicia una sesión de redirección de consola y aparece Video Viewer, es posible que deba de ajustar los controles siguientes a fin de ver y controlar el sistema remoto correctamente. Estos ajustes incluyen:

- Acceso a la barra de menú del visor
- El ajuste de la calidad de vídeo
- Sincronización de los apuntadores del mouse

Acceso a la barra de menú del visor

La barra de menú del visor es una barra de menú oculta. Para acceder a la barra de menú, mueva el cursor cerca del borde superior central de la ventana del escritorio de visor.

Asimismo, la barra de menú se puede activar al presionar la tecla de función predeterminada <F9>. Para reasignar esta tecla de función a una nueva función:

1. Presione <F9> o lleve el cursor a la parte superior de Video Viewer.
2. Presione la "tachuela" para fijar la barra de menú del visor.
3. En la barra de menú del visor, haga clic en **Herramientas** y seleccione **Opciones de sesión.**
4. En la ventana **Opciones de sesión**, haga clic en la ficha **General**.
5. En la ventana de la ficha **General** en el cuadro **Tecla de activación del menú**, haga clic en el menú desplegable y seleccione otra tecla de función.
6. Haga clic en **Aplicar** y después haga clic en **OK (Aceptar)**.

La Tabla 9-6 contiene las principales funciones que están disponibles para su uso en la barra de menú del visor.

Tabla 9-6. Selecciones de la barra de menú del visor

Elemento del menú	N.º	Descripción
Archivo	Capturar en archivo	Captura la pantalla actual del sistema remoto en un archivo **.bmp** (Windows) o **.png** (Linux) en el sistema local. Aparece un cuadro de diálogo que permite guardar el archivo en un lugar determinado.
	Salir	Cierra la página **Redirección de consola**.
Ver	Actualizar	Actualiza el puerto de visualización de la pantalla del sistema remoto.
	Pantalla completa	Amplía la pantalla de la sesión de ventana a pantalla completa.
Macros	Varios accesos directos de teclado	Ejecuta una combinación de teclas en el sistema remoto. Para conectar el teclado de la estación de administración al sistema remoto y ejecutar una macro: 1. Haga clic en **Herramientas**. 2. En la ventana **Opciones de sesión**, haga clic en la ficha General. 3. Seleccione **Pasar todas las pulsaciones de tecla al destino**. 4. Haga clic en **OK (Aceptar)**. 5. Haga clic en **Macros**. 6. En el menú **Macros**, haga clic en la combinación de teclas que desea ejecutar en el sistema de destino.
Herramientas	Ajuste automático de vídeo	Recalibra la salida de vídeo del visor de la sesión.
	Ajuste manual de vídeo	Muestra los controles individuales para ajustar manualmente la salida del visor de vídeo de la sesión. **NOTA:** El ajuste de la posición horizontal fuera del centro desincroniza los apuntadores del mouse.
	Opciones de sesión	Contiene ajustes adicionales de control del visor de sesión. La ficha **Mouse** permite seleccionar el sistema operativo que está usando para optimizar el funcionamiento del mouse en la redirección de consola. Seleccione **Windows**, **Linux** o **Ninguno**. La ficha **General** ofrece las siguientes opciones: • **Modo de paso de teclado:** seleccione **Pasar todas las pulsaciones de teclas al destino** para pasar las pulsaciones de tecla de la estación de administración al sistema remoto. • **Tecla de activación del menú**: selecciona la tecla de función que activa la barra de menú del visor. La ficha **Barra de herramientas** permite ajustar el tiempo **Retraso para ocultar la barra de herramientas** entre 1 y 10 segundos.
ayuda	N/D	Activa el menú **Ayuda**.

El ajuste de la calidad de vídeo

Video Viewer proporciona ajustes de vídeo que permiten optimizar el vídeo para obtener la mejor imagen posible. Haga clic en **Ayuda** para obtener más información.

Para ajustar automáticamente la calidad de vídeo:

1. Acceda a la barra de menú del visor. Consulte "Acceso a la barra de menú del visor".
2. Haga clic en **Herramientas** y seleccione **Ajuste automático de vídeo**.

La calidad de vídeo se recalibra y el visor de la sesión aparece nuevamente.

Para ajustar manualmente la calidad de vídeo:

1. Acceda a la barra de menú del visor. Consulte "Acceso a la barra de menú del visor".
2. Haga clic en **Herramientas** y seleccione **Ajuste manual de vídeo**.
3. En la ventana **Ajuste de vídeo**, haga clic en cada botón de ajuste de vídeo y ajuste los controles según sea necesario.

Cuando ajuste la calidad de vídeo manualmente, observe las siguientes directrices:

- Para evitar que los apuntadores de mouse se desincronicen, ajusten el valor horizontal de manera que la pantalla de escritorio del sistema remoto esté centrada en la ventana de la sesión.
- La reducción del valor de relación del ruido de los pixeles a cero ocasiona varios comandos de actualización de vídeo que generan un tráfico de red excesivo y vídeo parpadeante en la ventana de Video Viewer. Dell recomienda que ajuste el valor de la Proporción del ruido de los pixeles a un nivel que proporcione el rendimiento óptimo del sistema y mejore los pixeles, minimizando el tráfico de red.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema remoto Dell que usa la redirección de consola, la velocidad de aceleración del mouse en el sistema remoto puede no sincronizarse con el apuntador del mouse en la estación de administración, lo que ocasiona que aparezcan dos apuntadores de mouse en la ventana de Video Viewer.

Para sincronizar los apuntadores del mouse:

1. Acceda a la barra de menú del visor. Consulte "Acceso a la barra de menú del visor".
2. Haga clic en **Herramientas** y seleccione **Opciones de sesión**.
3. Haga clic en la ficha **Mouse**, seleccione el sistema operativo de la estación de administración y haga clic en **OK (Aceptar)**.
4. Haga clic en **Herramientas** y seleccione **Ajuste manual de vídeo**.
5. Ajuste los controles de horizontal de manera que la pantalla de escritorio del sistema remoto aparezca en el centro de la ventana de la sesión.
6. Haga clic en **OK (Aceptar)**.

Cuando se utiliza Linux (Red Hat® o Novell®), se usa la configuración predeterminada del mouse del sistema operativo para controlar la flecha del mouse en la pantalla de la redirección de consola del DRAC 5.

NOTA: En los sistemas Linux (Red Hat o Novell), hay problemas conocidos de sincronización de la flecha del mouse. Para minimizar los problemas de sincronización del mouse, asegúrese que todos los usuarios utilicen la configuración predeterminada del mouse.

Para obtener información sobre cómo desactivar la redirección de consola, consulte "Desactivación del KVM virtual remoto del DRAC 5".

Preguntas más frecuentes

¿La nueva sesión de vídeo de consola remota se puede iniciar cuando el vídeo local del servidor está desactivado?

Sí

¿Por qué tarda 15 segundos desactivar el vídeo local en el servidor después de solicitar la desactivación del mismo?

Esto da al usuario local la oportunidad de ejecutar alguna acción antes de que el vídeo se desactive.

¿Hay algún retraso al activar el vídeo local?

No, una vez que el DRAC 5 recibe la solicitud de activación del vídeo local, el vídeo se activa instantáneamente.

¿El usuario local también puede desactivar el vídeo?

Sí, el usuario local puede usar la CLI de racadm (local) para desactivar el vídeo.

¿El usuario local también puede activar el vídeo?

Sí, el usuario debe tener la CLI de racadm instalada en el servidor y sólo si el usuario puede acceder al servidor por medio de una conexión de RDP, por ejemplo, los servicios de terminal, Telnet o SSH. El usuario puede entonces iniciar sesión en el servidor y ejecutar racadm (local) para activar el vídeo.

Mi vídeo local está desactivado y por algún motivo no puedo acceder a mi DRAC 5 y no puedo acceder al servidor por medio de RDP, Telnet o SSH. ¿Cómo puedo recuperar el vídeo local?

La única forma de recuperar el video local en este caso es retirar el cable de alimentación de CA del servidor, agotar la alimentación del servidor y volver a conectar el cable de alimentación de CA. Esto hará que el video local vuelva a aparecer en el monitor del servidor. Asimismo, en la configuración del DRAC 5, la opción de video local cambiará a activada (valor predeterminado). El DRAC 5 deberá volver a configurarse si el video local debe desactivarse nuevamente.

¿La desactivación del vídeo local también desactiva el teclado y mouse locales?

No la desactivación del vídeo local sólo desactiva el vídeo proveniente del conector de salida del monitor del servidor; *no* desactiva el teclado y mouse que se conectan de manera local al servidor.

¿La desactivación del vídeo del servidor local desactiva el vídeo en la sesión vKVM remota?

No, la desactivación o activación del vídeo local es independiente de la sesión de consola remota.

¿Qué privilegios se necesitan para que un usuario de DRAC 5 active o desactive el vídeo del servidor local?

Los usuarios con privilegios de configuración de DRAC 5 pueden activar o desactivar el vídeo del servidor local.

¿Cómo se puede ver el estado actual del vídeo del servidor local?

El estado aparece en la página Configuración de la redirección de consola de la interfaz basada en web del DRAC 5. El comando racadm `getconfig -g cfgRacTuning` de la CLI de racadm muestra el estado en el objeto cfgRacTuneLocalServerVideo. El usuario local también puede ver el estado en la pantalla LCD del servidor como "Video OFF" (Vídeo desactivado) o como "Video OFF in 15" (Vídeo desactivado en 15).

¿Por qué algunas veces no veo el estado "Video OFF" (Vídeo desactivado) o "Video OFF in 15" (Vídeo desactivado en 15) en la pantalla LCD del servidor?

El estado del vídeo local es un mensaje de baja prioridad y se ocultará cuando se haya presentado un suceso de alta prioridad en el servidor. Los mensajes de la pantalla LCD se muestran según la prioridad; usted deberá resolver los mensajes de alta prioridad en la pantalla LCD y después de resolver o borrar el suceso, se mostrará el siguiente mensaje de baja prioridad. El mensaje del servidor de vídeo en la pantalla LCD es de naturaleza informativa.

¿Dónde puedo obtener más información sobre la función de vídeo del servidor local?

Visite el sitio Web de asistencia técnica de Dell en **support.dell.com** para acceder a un documento técnico que describe esta función.

Mi pantalla muestra el vídeo dañado. ¿Cómo resuelvo este problema?

En la ventana **Redirección de consola**, haga clic en **Actualizar** para actualizar la pantalla.

NOTA: Es posible que deba hacer clic en **Actualizar** varias veces para corregir los daños de vídeo.

Durante la redirección de consola, el teclado y el mouse se bloquean después de la hibernación en un sistema Windows 2000. ¿Qué provocó que esto ocurriera?

Para resolver este problema, restablezca el DRAC 5 por medio de la ejecución del comando **racadm racreset**.

No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola.

Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.

Durante la redirección de consola, el teclado y el mouse se bloquean después de la hibernación en un sistema Windows Server 2003. ¿Por qué ocurrió esto?

Para resolver este problema, seleccione un sistema operativo que no sea Windows para la aceleración del mouse desde el menú desplegable de la ventana de KVM virtual (vKVM), espere de 5 a 10 segundos y después seleccione Windows nuevamente. Si el problema no se resuelve, deberá restablecer el DRAC 5 por medio del comando **racadm racreset**.

Si el problema sigue sin resolverse, deberá restablecer el DRAC 5 por medio del comando **racadm racreset hard**.

¿Por qué no funcionan el teclado y mouse de vKVM?

Debe establecer el controlador de USB en **Activado con compatibilidad de BIOS** en la configuración del BIOS del sistema administrado. Reinicie el sistema administrado y presione <F2> para ingresar a la configuración. Seleccione **Dispositivos integrados** y después seleccione **Controlador USB**. Guarde los cambios y reinicie el sistema.

¿Por qué la pantalla de la consola del sistema administrado aparece en blanco cuando Windows muestra una pantalla azul de error?

El sistema administrado no tiene el controlador de vídeo ATI correcto. Debe actualizar el controlador de video con el DVD *Dell Systems Management Tools and Documentation*.

¿Por qué aparece una pantalla en blanco en la consola remota después de terminar la instalación de Windows 2000?

El sistema administrado no tiene el controlador de vídeo ATI correcto. La redirección de consola del DRAC 5 no se ejecutará correctamente en el controlador de vídeo SVGA en el CD de distribución de Windows 2000. Debe instalar Windows 2000 con el DVD *Dell Systems Management Tools and Documentation* para asegurarse de contar con los controladores más recientes compatibles con el sistema administrado.

¿Por qué aparece una pantalla en blanco en el sistema administrado al cargar el sistema operativo Windows 2000?

El sistema administrado no tiene el controlador de vídeo ATI correcto. Debe actualizar el controlador de video por medio del DVD *Dell Systems Management Tools and Documentation*.

¿Por qué aparece una pantalla en blanco en el sistema administrado en la ventana de DOS de pantalla completa de Windows?

El sistema administrado no tiene el controlador de vídeo ATI correcto. Debe actualizar el controlador de video por medio del DVD *Dell Systems Management Tools and Documentation*.

¿Por qué no puedo ingresar a la configuración del BIOS cuando presiono la tecla <F2>?

Esta conducta es típica en un entorno Windows. Utilice el mouse para hacer clic en un área de la ventana de la redirección de consola para ajustar el enfoque. Para mover el enfoque hacia la barra de menú inferior de la ventana de redirección de consola, utilice el mouse y haga clic en uno de los objetos de la barra de menú inferior.

¿Por qué no se sincroniza el mouse vKVM cuando utilizo el DVD Dell Systems Management Tools and Documentation para instalar de manera remota el sistema operativo?

Configure la redirección de consola del sistema operativo que se está ejecutando en el sistema de destino.

1. En el menú de la barra de herramientas de vKVM, haga clic en **Herramientas** y seleccione **Opciones de sesión**.
2. En la ventana **Opciones de sesión**, haga clic en la ficha **Mouse**.
3. En el cuadro **Aceleración del mouse**, seleccione el sistema operativo que se ejecuta en el sistema de destino y haga clic en **OK (Aceptar)**.

¿Por qué el mouse vKVM no se sincroniza después de regresar del modo de hibernación en un sistema Windows?

Seleccione otro sistema operativo para la aceleración del mouse en el menú desplegable de la ventana de vKVM. A continuación, regrese al sistema operativo original para inicializar el dispositivo de mouse USB.

1. En la barra de herramientas de vKVM, haga clic en **Herramientas** y seleccione **Opciones de sesión**.
2. En la ventana **Opciones de sesión**, haga clic en la ficha **Mouse**.
3. En el cuadro **Aceleración del mouse**, seleccione otro sistema operativo y haga clic en **OK (Aceptar)**.
4. Inicialice el dispositivo de mouse USB.

¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la redirección de consola?

El BIOS de Dell emula el controlador de mouse como mouse PS/2. Debido al diseño, el mouse PS/2 utiliza la posición relativa para el apuntador de mouse, lo que ocasiona un retraso en la sincronización. El DRAC 5 tiene un controlador de mouse USB, que permite la posición absoluta y un seguimiento más preciso del apuntador del mouse. Aun cuando el DRAC 5 pasara la posición absoluta del mouse USB al BIOS de Dell, la emulación de BIOS lo convertiría nuevamente a la posición relativa y el comportamiento sería el mismo.

¿Por qué no se sincroniza el mouse en la consola de texto de Linux?

El KVM virtual necesita el controlador de mouse USB, pero el controlador de mouse USB sólo está disponible en el sistema operativo X-Window.

Aún tengo problemas con la sincronización del mouse.

Compruebe que la pantalla del escritorio del sistema de destino esté centrada en la ventana de la redirección de consola.

1. En la barra de herramientas de vKVM, haga clic en **Herramientas** y seleccione **Ajuste manual de vídeo**.
2. Ajuste los controles horizontal y vertical según sea necesario para alinear el escritorio en la ventana de redirección de consola.
3. Haga clic en **Close (Cerrar)**.
4. Mueva el cursor del mouse del sistema de destino a la esquina superior izquierda de la ventana de la redirección de consola y después mueva el cursor nuevamente al centro de la ventana.
5. Repita los pasos 2 a 4 hasta que los cursores se sincronicen.

¿Por qué e mouse y teclado de vKVM no funcionan cuando se cambia la aceleración del mouse en distintos sistemas operativos?

El teclado y mouse USB de vKVM están inactivos de 5 a 10 segundos después de cambiar la aceleración del mouse. Algunas veces, la carga de la red ocasiona que esta operación tarde más de lo normal (más de 10 segundos).

¿Por qué no puedo ver la parte inferior de la pantalla del servidor en la ventana de vKVM?

Asegúrese que la resolución de la pantalla del servidor es de 1280 x 1024 píxeles a 60 Hz con 128 colores.

¿Por qué no puedo usar un teclado o mouse al instalar un sistema operativo de Microsoft® de manera remota por medio de la redirección de consola del DRAC 5?

Cuando instala un sistema operativo admitido de Microsoft de manera remota en un sistema con redirección de consola activada en el BIOS, aparece un mensaje de conexión EMS que solicita que seleccione **OK (Aceptar)** para poder continuar. Usted no puede usar el mouse para seleccionar **OK (Aceptar)** de manera remota. Debe seleccionar **OK (Aceptar)** en el sistema local o reiniciar el sistema administrado de manera remota, reinstalar y después desactivar la redirección de consola en el BIOS.

Microsoft genera este mensaje para avisar al usuario que la redirección de consola está activada. Para asegurar que este mensaje no aparece, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.

¿Por qué la redirección de consola no muestra el menú de inicio del sistema operativo en las versiones china, japonesa y coreana de Microsoft Windows 2000?

En los sistemas que ejecutan Windows 2000 que pueden iniciar varios sistemas operativos, cambie el sistema operativo predeterminado de inicio por medio de los siguientes pasos:

1. Haga clic con el botón derecho del mouse en el icono **Mi PC** y seleccione **Propiedades**.
2. Haga clic en la ficha **Opciones avanzadas**.
3. Haga clic en **Inicio y recuperación**.
4. Seleccione el nuevo sistema operativo predeterminado en la lista **Inicio**.
5. En el cuadro **Mostrar la lista durante**, escriba el número de segundos que desea que se muestre la lista de opciones antes de que el sistema operativo predeterminado se inicie automáticamente.

¿Por qué el indicador de Bloq Núm de mi estación de administración no muestra el estado de Bloq Núm en el servidor remoto?

Al acceder al indicador de Bloq Núm por medio del DRAC 5, el indicador no necesariamente coincide con el estado de Bloq Núm en el servidor remoto. El estado de Bloq Núm depende de la configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Núm en la estación de administración.

¿Por qué aparecen varias ventanas del visor de sesión cuando establezco una sesión de redirección de consola?

Usted está configurando una sesión de redirección de consola en el sistema local. Vuelva a configurar la sesión en un sistema remoto.

Si ejecuto una sesión de redirección de consola y un usuario local accede al sistema remoto, ¿recibiré un mensaje de advertencia?

No Si un usuario local accede al sistema, dicho usuario podrá anular las acciones de usted sin que usted reciba una advertencia.

¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?

Dell recomienda una conexión de 5 MB/s para un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.

¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la redirección de consola?

La estación de administración requiere un procesador Intel Pentium III a 500 MHz con un mínimo de 256 MB de RAM.

Cuál es el número máximo de sesiones de redirección de consola que puedo ejecutar en un sistema remoto?

El DRAC 5 admite hasta dos sesiones simultáneas de redirección de consola.

¿Por qué tengo problemas con la sincronización del mouse?

En los sistemas Linux (Red Hat o Novell), hay problemas conocidos de sincronización de la flecha del mouse. Para minimizar los problemas de sincronización del mouse, asegúrese que todos los usuarios utilicen la configuración predeterminada del mouse.

¿Cómo puedo instalar un explorador de web en mi estación de administración que tiene un sistema de archivos de sólo lectura?

Si está ejecutando Linux y la estación de administración tiene un sistema de archivos de sólo lectura, se puede instalar un explorador en un sistema cliente sin requerir una conexión al DRAC 5. Si utiliza el paquete de instalación nativo del complemento, el explorador se puede instalar manualmente durante la fase de configuración del cliente.

AVISO: En un entorno de cliente de sólo lectura, si el firmware del DRAC 5 se actualiza con una versión más reciente del complemento, el complemento VM instalado no funcionará. Esto se debe a que las funciones del complemento anterior no tienen permiso de funcionar cuando el firmware contiene una versión más reciente del complemento. En este caso, se pedirá la instalación de complemento en el cliente. Como el sistema de archivos es de sólo lectura, la instalación fallará y las funciones del complemento no estarán disponibles.

Para obtener el paquete de instalación del complemento:

1. Inicie sesión en un DRAC 5 existente.
2. Cambie el URL en la barra de dirección del explorador, de:

   ```
   https://<IP_del_RAC>/cgi-bin/webcgi/main
   ```

   a:

   ```
   https://<IP_del_RAC>/plugins/ # Be sure to include the trailing slash. (Asegúrese de incluir la última diagonal.)
   ```

3. Note que hay dos subdirectorios vm y vkvm. Desplácese hacia el subdirectorio correspondiente, haga clic con el botón derecho del mouse en el archivo rac5XXX.xpi y seleccione Guardar destino como....
4. Elija una ubicación para guardar el archivo del paquete de instalación del complemento.

Para instalar el paquete de instalación del complemento:

1. Copie el paquete de instalación en el recurso compartido del sistema de archivos nativo del cliente que esté accesible para el cliente.
2. Abra una instancia del explorador en el sistema cliente.
3. Introduzca la ruta de acceso del archivo del paquete de instalación del complemento en la barra de dirección del explorador. Por ejemplo,

   ```
   file:///tmp/rac5vm.xpi
   ```

4. El explorador guiará al usuario a través de la instalación del complemento.

Una vez instalado, el explorador no volverá a solicitar la instalación del complemento, siempre y cuando el firmware del DRAC 5 de destino no tenga una versión más reciente del complemento.

¿Por qué la sesión de redirección de consola finaliza cuando reinicio mi terminal?

Cuando la tarjeta de interfaz de red (NIC) del DRAC 5 está en modo compartido o compartido con protección contra fallas, el restablecimiento del sistema hace que también se restablezca la LAN de la placa base (LOM). En las redes cuyos conmutadores cuentan con el protocolo de árbol de extensión STP (Spanning Tree Protocol) activado, esto hace que la conexión entre la estación de administración y el cliente se restablezca después de diez a quince segundos aproximadamente. En consecuencia, se pierde la conectividad con el sistema remoto y aparece un mensaje de error en los clientes de medios virtuales y redirección de consola. Si accede a la interfaz del usuario del DRAC en este momento, recibirá un mensaje de error que indica que no se encontró la página.

Para resolver este inconveniente:

- Utilice la tarjeta de interfaz de red dedicada del DRAC 5 para establecer conexión a través de la red.
- Desactive el protocolo STP en los conmutadores de red.

Regresar a la página de contenido

Regresar a la página de contenido

Glosario

Dell™ Remote Access Controller 5 Guía del usuario del firmware versión 1.40

Active Directory

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

AGP

Siglas de accelerated graphics port (puerto de gráficos acelerados), que es una especificación de bus que permite que las tarjetas de gráficos accedan 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 para American Standard Code for Information Interchange (Código estándar estadounidense para intercambio de información), que es una representación de códigos que se usa para mostrar o imprimir letras, números y otros caracteres.

BIOS

Siglas de basic input/output system (sistema básico de entradas y salidas), que es la parte del software de sistema que proporciona la interfaz al nivel más bajo a los dispositivos periféricos y que controla la primera fase del proceso de inicio del sistema, incluyendo la instalación del sistema operativo en la memoria.

BMC

Siglas de baseboard management controller (controlador de administración de la placa base), que es la interfaz de controlador entre el DRAC 5 y el BMC del sistema administrado.

bus

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

CA

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

captura SNMP

Notificación (suceso) generada por el DRAC 5 o el BMC que contiene información sobre los cambios de estado en el sistema administrado o sobre problemas potenciales de hardware.

CD

Siglas de compact disc (disco compacto).

CHAP

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

CIM

Siglas de Common Information Model (Modelo de información común), que es un marco de trabajo diseñado para la administración de sistemas en una red.

CLI

Siglas de command-line interface (interfaz de línea de comandos).

CLP

Siglas de command-line protocol (protocolo de línea de comandos).

CSR

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

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 DRAC 5 mantiene un disco RAM en su memoria.

DDNS

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

DLL

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

DMTF

Siglas de Distributed Management Task Force (Equipo de trabajo de administración distribuida).

DNS

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

DRAC 5

Siglas de Dell Remote Access Controller 5.

DSU

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

esquema ampliado

Una solución que se usa con Active Directory para determinar el acceso de usuario al DRAC 5; utiliza objetos de Active Directory definidos por Dell.

esquema estándar

Solución que se usa con Active Directory para determinar el acceso de usuario al DRAC 5; utiliza exclusivamente objetos de grupo de Active Directory.

Estación de administración

La estación de administración es un sistema que accede de manera remota al DRAC 5.

FQDN

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

FSMO

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

GMT

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

GPIO

Abreviatura de general purpose input/output (entrada/salida de propósito general).

GRUB

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

GUI

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

hardware log

Registra los sucesos generados por el DRAC 5 y el BMC.

ICMB

Abreviatura de Intelligent Chassis Management Bus (bus de administración de chasis 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).

IP

Abreviatura de Internet Protocol (protocolo de Internet), que es un nivel de red de TCP/IP. El IP proporciona enrutamiento, fragmentación y reensamblaje de paquetes.

IPMB

Siglas de intelligent platform management bus (bus de administración de inteligentes), que es un bus que se utiliza en la tecnología de administración de sistemas.

IPMI

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

Kbps

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

LAN

Abreviatura de local area network (red de área local).

LDAP

Abreviatura de protocolo ligero de acceso a directorios.

LED

Abreviatura de diodo emisor de luz.

LOM

Abreviatura de local area network on motherboard (red de área local integrada a la placa base).

MAC

Siglas de media access control (control de acceso a medios), que es un subnivel de red entre un nodo de red y el nivel físico de la red.

MAP

Siglas de Manageability Access Point (Punto de acceso de administrabilidad).

Mbps

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

MIB

Abreviatura de management information base (base de información de administración).

MII

Siglas de Media Independent Interface (Interfaz independiente de medios).

NAS

Abreviatura de network attached storage (almacenamiento conectado a red).

NIC

Siglas de network interface card (tarjeta de interfaz de red). Una placa adaptadora de circuitos instalada en un equipo para brindar una conexión física con la red.

OID

Abreviatura de Object Identifiers (identificadores de objeto).

PCI

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

PKI

Siglas de Public Key Infrastructure (Infraestructura de clave pública). La PKI permite que los usuarios de una red pública no segura como la Internet para intercambiar datos de manera segura y privada mediante el uso de un par de claves criptográficas (una pública y una privada) que se obtiene y comparte por medio de una autoridad de confianza.

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.

RAM

Siglas de memoria de acceso aleatorio. La RAM es una memoria de uso general que se puede leer y en la que se puede escribir en los sistemas y en el DRAC 5.

RAC

Abreviatura de remote access controller (controlador de acceso remoto).

redirección de consola

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

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 en la instalación de paquetes de software. Es similar a un programa de instalación.

SAC

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

SAI

Abreviatura de sistema de energía ininterrumpida.

SAP

Siglas de Service Access Point (Punto de acceso de servicio).

SEL

Siglas de registro de sucesos del sistema.

sistema administrado

El sistema administrado es el sistema en el que se instala o incorpora el DRAC 5.

SMI

Abreviatura de systems management interrupt (interrupción de administración del sistema).

SMTP

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

SMWG

Siglas de Systems Management Working Group (Grupo de trabajo de administración de sistemas).

SNMP

Abreviatura de Simple Network Management Protocol (protocolo simple de administración de redes), que es un protocolo diseñado para administrar nodos en una red de IP. Los DRAC 5 son dispositivos administrados (nodos) de SNMP.

SSH

Abreviatura para Secure SHell.

SSL

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

TAP

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

TCP/IP

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

TFTP

Abreviatura de Trivial File Transfer Protocol (protocolo trivial de transferencia de archivos, que es un protocolo de transferencia simple usado para cargar

código de inicio a los dispositivos o sistemas sin discos.

USB

Abreviatura de bus serial universal.

UTC

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

VLAN

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

VNC

Abreviatura de virtual network computing (cómputo de red virtual).

VT-100

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

WAN

Abreviatura de wide area network (red de área amplia).

Regresar a la página de contenido