

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

[Descripción de DRAC 5](#)
[Instalación y configuración de DRAC 5](#)
[Configuración y uso de la consola de línea de comandos del DRAC 5](#)
[Configuración del DRAC 5 por medio de la interfaz de usuario por web](#)
[Recuperación y solución de problemas del sistema administrado](#)
[Uso del DRAC 5 con Microsoft Active Directory](#)
[Uso de la redirección de consola con interfaz gráfica de usuario](#)
[Uso y configuración de medios virtuales](#)
[Uso de la interfaz de línea de comandos de RACADM](#)
[Instalación del sistema operativo por medio de VM-CLI](#)
[Uso de la interfaz de línea de comandos de SM-CLP del DRAC 5](#)
[Solución de problemas](#)
[Descripción de subcomandos de RACADM](#)
[Definiciones de grupos y objetos de la base de datos de propiedades de DRAC 5](#)
[Interfases de RACADM admitidas](#)
[Glosario](#)

Notas, avisos y precauciones

-  **NOTA:** Una NOTA indica información importante que ayuda a hacer mejor uso del equipo.
 -  **AVISO:** Un AVISO indica la posibilidad de daños al hardware o pérdida de datos y le explica cómo evitar el problema.
 -  **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños a la propiedad, lesiones personales o muerte.
-

La información contenida en este documento puede modificarse sin previo aviso.
© 2006 Dell Inc. Todos los derechos reservados.

Queda estrictamente prohibida la reproducción de este documento en cualquier forma sin la autorización por escrito de Dell Inc.

Las marcas comerciales usadas en este texto: *Dell*, el logotipo de *DELL*, *Dell OpenManage* y *PowerEdge*, son marcas comerciales registradas de Dell Inc.; *Microsoft* y *Windows* son marcas comerciales registradas y *Windows Server* es una marca comercial de Microsoft Corporation; *Red Hat* es una marca comercial registrada de Red Hat, Inc.; *Intel* es una marca comercial registrada de Intel Corporation; *UNIX* es una marca comercial registrada de The Open Group en los Estados Unidos y en otros países.

Copyright 1998-2006 The OpenLDAP Foundation. Todos los derechos reservados. Sólo se permite la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, según lo autoriza la licencia pública de OpenLDAP. Una copia de esta licencia está disponible en el archivo LICENSE en el directorio principal de la distribución, o bien, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Otros pueden obtener copyright de los archivos individuales y/o los paquetes contribuidos y estos pueden quedar sujetos a restricciones adicionales. Este trabajo proviene de la distribución de la versión 3.3 de LDAP de la Universidad de Michigan. Este trabajo también contiene materiales provenientes de fuentes públicas. Se puede obtener información de OpenLDAP en <http://www.OpenLDAP.org/>. Portions Copyright 1998-2004 Kurt D. Zellenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. Todos los derechos reservados. Sólo se permite la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, según lo autoriza la licencia pública de OpenLDAP. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. Todos los derechos reservados. Se permite la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, a condición de que este aviso se conserve. Los nombres de los titulares de copyright no pueden ser usados para respaldar o promover productos provenientes de este software sin el previo permiso específico por escrito. Este software se ofrece "tal cual" sin garantías explícitas ni implícitas. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. Todos los derechos reservados. Se permite la redistribución y el uso en las formas de código fuente y binaria con la condición de que este aviso se conserve y que se dé el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se puede usar para respaldar o promover productos provenientes de este software sin el previo permiso específico por escrito. Este software se ofrece "tal cual" sin garantías explícitas ni implícitas. Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc., renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc., renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Abril de 2006 Rev. A01

[Regresar a la página de contenido](#)

Descripción de subcomandos de RACADM

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [help](#)
- [arp](#)
- [clearasrscreen](#)
- [config](#)
- [getconfig](#)
- [coredump](#)
- [coredumpdelete](#)
- [fwupdate](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getractable](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [setniccfg](#)
- [getniccfg](#)
- [getsvctag](#)
- [racdump](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [getraclog](#)
- [cirraclog](#)
- [getsel](#)
- [cirsel](#)
- [gettracelog](#)
- [sslcsngen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [vmkey](#)

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

help

 **NOTA:** Para usar este comando, usted 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 | Enumera todos los subcomandos disponibles para usarse con racadm y proporciona una breve descripción de cada uno. |

Sinopsis

```
racadm help
```

```
racadm help <subcomando>
```

Descripción

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

Salida

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

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

arp

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

La [tabla A-2](#) describe el comando **arp**.

Tabla A-2. Comando arp

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

Sinopsis

```
racadm arp
```

Interfaces admitidas

- 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

cleararscreen

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

La [tabla A-3](#) describe el subcomando **cleararscreen**.

Tabla A-3. cleararscreen

| Subcomando | Definición |
|---------------|--|
| cleararscreen | Borra la última pantalla de colisión que está en la memoria. |

Sinopsis

```
racadm cleararscreen
```

Interfaces admitidas

- 1 RACADM local
 - 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

config

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

La [tabla A-4](#) describe 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] -f <nombre_de_archivo>
```

```
racadm config -g <nombre de grupo> -o <nombre de objeto> [-i <índice>] <Valor>
```

Interfaces admitidas

- | RACADM local
- | RACADM remoto
- | RACADM de conexión Telnet/SSH/serie

Descripción

El subcomando **config** permite al usuario establecer parámetros de configuración de DRAC 5 individualmente o procesarlos en lote como parte de un archivo de configuración. Si la información es diferente, ese objeto de DRAC 5 se escribe con el nuevo valor.

Entrada

La [tabla A-5](#) describe las opciones del subcomando **config**.

 **NOTA:** Las opciones **-f** y **-p** no se admiten en la consola de conexión serie/Telnet/SSH.

Tabla A-5. Opciones y descripciones del subcomando config.

| Opción | Descripción |
|--------|--|
| -f | La opción -f <nombre de archivo> hace que config lea el contenido del archivo especificado con el <nombre de archivo> y que configure el DRAC 5. El archivo debe contener los datos en el formato especificado en " Reglas de análisis ". |
| -p | La opción -p , u opción de contraseña, indica a config que borre las anotaciones de contraseñas contenidas en el archivo config -f <nombre de archivo> después de que se completa la configuración. |
| -g | La opción -g <nombre de grupo> , 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 establecer. |
| -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 "nombrado". |
| -c | La opción -c , u opción de verificación, se usa con el subcomando config y permite al usuario analizar el archivo .cfg para encontrar errores de sintaxis. Si se encuentran errores, se muestra el número de línea y una breve descripción del error. No se realizan las operaciones de escritura en el DRAC 5. Esta opción es sólo un control. |

Salida

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

- | Sintaxis, nombre de grupo, nombre de objeto o índice inválido, u otros miembros inválidos de la base de datos
- | Fallas de la CLI de racadm

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

Ejemplos

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

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

```
| racadm config -f myrac.cfg
```

Configura o reconfigura el DRAC 5. El archivo **myrac.cfg** se puede crear con el comando **getconfig**. El archivo **myrac.cfg** también se puede editar manualmente, siempre y cuando se sigan las reglas de análisis.

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

getconfig

Descripción del subcomando getconfig

El subcomando **getconfig** permite al usuario recuperar parámetros de configuración de DRAC 5 individualmente, o se pueden recuperar todos los grupos de configuración del RAC y guardarse en un archivo.

Entrada

La [tabla A-6](#) describe las opciones del subcomando **getconfig**.

 **NOTA:** La opción **-f** mostrará el contenido del archivo en la pantalla de la terminal en vez de escribirlo a un archivo, ya que ningún sistema de archivo está disponible.

Tabla A-6. Opciones del subcomando getconfig

| Opción | Descripción |
|--------|---|
| -f | La opción -f indica al comando getconfig que escriba toda la configuración del RAC en un archivo de configuración. Este archivo se puede usar para realizar operaciones de configuración de procesamiento en lote por medio del subcomando config . NOTA: La opción -f no crea anotaciones para los grupos cfglpmiPet y cfglpmiPef . Usted debe establecer al menos un destino de captura para capturar el grupo cfglpmiPet en el archivo. |
| -g | La opción -g <nombre_de_grupo> , u opción group , se puede usar para mostrar la configuración de un solo grupo. El nombre de grupo es el nombre del grupo usado en los archivos racadm.cfg . Si el grupo es un grupo indexado, use la opción -i . |
| -h | La opción -h o help , muestra una lista de todos los grupos de configuración disponibles que puede utilizar. Esta opción es útil cuando usted no recuerda los nombres exactos de los grupos. |
| -i | La opción -i <índice> , u opción index , 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 -i <índice> no se especifica, se asumirá un valor de 1 para los grupos, que son tablas que tienen varias anotaciones. El índice se especifica aquí mediante el valor del índice; no mediante un valor "nombrado". |
| -o | La opción -o <nombre_de_objeto> u opción de objeto especifica el nombre de objeto que se usa en la consulta. Esta opción es optativa y se puede usar con la opción -g . |
| -u | La opción -u <nombre_de_usuario> , u opción user name , 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 con la pantalla de propiedades y se usa con la opción -g . |

Salida

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

- 1 Sintaxis, nombre de grupo, nombre de objeto o índice inválido, u otros miembros inválidos de la base de datos
- 1 Fallas de transporte de la CLI de **racadm**

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

Ejemplos

```
1 racadm getconfig -g cfgLanNetworking
```

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

```
1 racadm getconfig -f myrac.cfg
```

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

```
1 racadm getconfig -h
```

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

```
1 racadm getconfig -u root
```

Muestra las propiedades de configuración del usuario "root".

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

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

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>
racadm getconfig -g <nombre de grupo> [-i <indice>]
racadm getconfig -u <nombre de usuario>
racadm getconfig -h
```

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

coredump

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

La [tabla A-7](#) describe el subcomando **coredump**.

Tabla A-7. **coredump**

| Subcomando | Definición |
|-----------------|---|
| coredump | Muestra el último volcado central del DRAC 5. |

Sinopsis

```
racadm coredump
```

Descripción

El subcomando **coredump** muestra información detallada relacionada con cualquier problema crítico reciente que haya ocurrido en el RAC. La información de vaciado del registro de la CPU se puede usar para diagnosticar estos problemas críticos.

De estar disponible, la información de vaciado de registro de la CPU persiste a pesar de los ciclos de encendido del RAC y permanecerá disponible hasta que cualquiera de las siguientes condiciones ocurra:

- 1 La información de vaciado de registro de la CPU se borra con el subcomando **coredumpdelete**.
- 1 Se presenta otra condición crítica en el RAC. En este caso, la información de vaciado de registro de la CPU estará relacionada con el último error crítico que se presentó.

Consulte el subcomando **coredumpdelete** para obtener más información sobre cómo borrar el contenido de **coredump**.

Interfaces admitidas

- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

 **NOTA:** La opción **-f** no se admite en la interfaz de RACADM por Telnet/SSH/serie.

coredumpdelete

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

La [tabla A-8](#) describe el subcomando `coredumpdelete`.

Tabla A-8. `coredumpdelete`

| Subcomando | Definición |
|-----------------------------|---|
| <code>coredumpdelete</code> | Borra el volcado central almacenado en el DRAC 5. |

Sinopsis

```
racadm coredumpdelete
```

Descripción

El subcomando `coredumpdelete` se puede usar para limpiar los datos actuales que residan en el registro de `coredump` y que estén almacenados en el RAC.

 **NOTA:** Si se ejecuta un comando `coredumpdelete` y no hay un registro de `coredump` almacenado actualmente en el RAC, el comando mostrará un mensaje de ejecución satisfactoria. Este comportamiento es el esperado.

Consulte el subcomando `coredump` para obtener más información acerca de cómo ver el registro de `coredump`.

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

fwupdate

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

 **NOTA:** Antes de comenzar con la actualización del firmware, consulte "[Actualización del firmware del DRAC 5](#)" para obtener más instrucciones..

La [tabla A-9](#) describe el subcomando `fwupdate`.

Tabla A-9. `fwupdate`

| Subcomando | Definición |
|-----------------------|-----------------------------------|
| <code>fwupdate</code> | Actualiza el firmware del DRAC 5. |

Sinopsis

```
racadm fwupdate -s
```

```
racadm fwupdate -g -u -a <TFTP_Server_IP_Address> -d <path>
```

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

Descripción

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

- 1 Revisar el estado del proceso de actualización del firmware
- 1 Actualizar el firmware del DRAC 5 a partir de un servidor TFTP y proporcionando una dirección IP y una ruta opcional
- 1 Actualizar el firmware del DRAC 5 a partir del sistema local de archivos por medio de la utilidad RACADM local

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

Entrada

La [tabla A-10](#) describe las opciones del subcomando **fwupdate**.

 **NOTA:** La opción **-p** se admite únicamente en el RACADM local y no es compatible con la consola serie/Telnet/SSH.

Tabla A-10. Opciones del subcomando fwupdate

| Opción | Descripción |
|--------|---|
| -u | La opción de actualización realiza una suma de comprobación del archivo de actualización del firmware e inicia el proceso de actualización real. Esta opción se puede usar junto con las opciones -g o -p . Al final de la actualización, el DRAC 5 realiza un restablecimiento ordenado. |
| -s | La opción de estado indica el estado actual de dónde se encuentra en el proceso de actualización. Esta opción siempre se utiliza sola. |
| -g | La opción get indica al firmware que obtenga el archivo de actualización de firmware del servidor TFTP. El usuario también debe especificar las opciones -a y -d . En ausencia de la opción -a , los valores predeterminados se leen de las propiedades contenidas en el grupo cfgRemoteHosts , usando las propiedades cfgRhostsFwUpdateIpAddr y cfgRhostsFwUpdatePath . |
| -a | La opción dirección IP especifica la dirección de IP del servidor TFTP. |
| -d | La opción -d o directorio especifica el directorio del servidor TFTP o del servidor host del DRAC 5 donde reside el archivo de actualización del firmware. |
| -p | La opción -p o put , se usa cuando para actualizar el archivo de firmware del sistema administrado al DRAC 5. La opción -u se debe usar con la opción -p . |

Salida

Muestra un mensaje que indica qué operación se está realizando.

Ejemplos

```
1 racadm fwupdate -g -u -a 143.166.154.143 -d <path>
```

En este ejemplo, la opción **-g** le indica al firmware que descargue el archivo de actualización del firmware desde una ubicación (especificada por la opción **-d**) en el servidor TFTP, en una dirección IP específica (que se indica con la opción **-a**). Una vez que el archivo de imagen haya sido descargado del servidor TFTP, se iniciará el proceso de actualización. Cuando concluya, el DRAC 5 se restablecerá.

```
1 racadm fwupdate -s
```

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

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

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

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

En este ejemplo, RACADM se usa de manera remota para actualizar el firmware del DRAC especificado con el nombre de usuario y la contraseña del DRAC proporcionados. La imagen se obtiene de un servidor TFTP.

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

getssninfo

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

La [tabla A-11](#) describe el subcomando **getssninfo**.

Tabla A-11. Subcomando getssninfo

| Subcomando | Definición |
|------------|------------|
|------------|------------|

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

Sinopsis

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

Descripción

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

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

Entrada

La [tabla A-12](#) describe las opciones del subcomando **getssninfo**.

Tabla A-12. Opciones del subcomando **getssninfo**

| Opción | Descripción |
|--------|--|
| -A | La opción -A elimina la impresión de los encabezados de los datos. |
| -u | La opción de nombre de usuario -u <nombre de usuario> limita la salida impresa a sólo 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 se imprime cuando se especifica esta opción. |

Ejemplos

```
1 racadm getssninfo
```

La [tabla A-13](#) ofrece un ejemplo del mensaje de salida generado por el comando **racadm getssninfo**.

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

| Usuario | Dirección IP | Tipo | Consolas |
|---------|--------------|--------|-------------|
| root | 192.168.0.10 | Telnet | KVM virtual |

```
1 racadm getssninfo -A
"root" 143.166.174.19 "Telnet" "NONE"
1 racadm getssninfo -A -u *
"root" "143.166.174.19" "Telnet" "NONE"
"bob" "143.166.174.19" "GUI" "NONE"
```

getsysinfo

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

La [tabla A-14](#) describe las opciones del subcomando `racadm getsysinfo`.

Tabla A-14. `getsysinfo`

| Comando | Definición |
|-------------------------|---|
| <code>getsysinfo</code> | Muestra información de DRAC 5, información del sistema e información del estado del circuito de vigilancia. |

Sinopsis

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

Descripción

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

Entrada

La [tabla A-15](#) describe las opciones del subcomando `getsysinfo`.

Tabla A-15. Opciones del subcomando `getsysinfo`

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

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

Salida

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

```
l 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"

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

getractime

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

La [tabla A-16](#) describe el subcomando `getractime`.

Tabla A-16. `getractime`

| Subcomando | Definición |
|-------------------------|--|
| <code>getractime</code> | Muestra la hora actual del controlador de acceso remoto. |

Sinopsis

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

Descripción

El subcomando `getractime` muestra la hora en el formato siguiente:

```
l d: la cadena yyyymmddhhmmss.mmssmmss sin opciones aparece en el mismo formato que el comando date de UNIX.
```

Salida

El subcomando `getractive` muestra la salida en una línea.

Ejemplo del mensaje de salida

```
racadm getractive
Thu Dec 8 20:15:26 2005
racadm getractive -d
20051208201542.000000
```

Interfaces admitidas

- | RACADM local
 - | RACADM remoto
 - | RACADM de conexión Telnet/SSH/serie
-

ifconfig

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

La [tabla A-17](#) describe el subcomando `ifconfig`.

Tabla A-17. `ifconfig`

| Subcomando | Definición |
|-----------------------|--|
| <code>ifconfig</code> | Muestra el contenido de la tabla de interfaz de red. |

Sinopsis

```
racadm ifconfig
```

netstat

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

La [tabla A-18](#) describe el subcomando `netstat`.

Tabla A-18. `netstat`

| Subcomando | Definición |
|----------------------|---|
| <code>netstat</code> | Muestra la tabla de encaminamiento y las conexiones actuales. |

Sinopsis

```
racadm netstat
```

Interfaces admitidas

- | RACADM remoto
 - | RACADM de conexión Telnet/SSH/serie
-

ping

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

La [tabla A-19](#) 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. Se envía un paquete de eco ICMP a la dirección IP de destino, según el contenido actual de la tabla de enrutamiento. |

Sinopsis

```
racadm ping <dirección_IP>
```

Interfaces admitidas

- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

setniccfg

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

La [tabla A-20](#) describe el subcomando **setniccfg**.

Tabla A-20. setniccfg

| Subcomando | Definición |
|------------|--|
| setniccfg | Establece la configuración IP para el controlador. |

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

Sinopsis

```
racadm setniccfg -d
```

```
racadm setniccfg -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.

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

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

- 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 separadas con puntos.

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

Salida

Si la operación no se realizó satisfactoriamente, el subcomando `setniccfg` mostrará un mensaje de error correspondiente. Si se realiza satisfactoriamente, aparecerá un mensaje.

Interfaces admitidas

- 1 RACADM local
 - 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

getniccfg

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

La [tabla A-21](#) describe los subcomandos `setniccfg` y `getniccfg`.

Tabla A-21. `setniccfg/getniccfg`

| Subcomando | Definición |
|------------------------|---|
| <code>getniccfg</code> | 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 se ejecuta satisfactoriamente, el subcomando `getniccfg` mostrará un mensaje de error correspondiente. De lo contrario, cuando se ejecute satisfactoriamente, el mensaje aparecerá en el formato siguiente:

```
NIC Enabled      = 1
DHCP Enabled     = 1
IP Address       = 192.168.0.1
Subnet Mask      = 255.255.255.0
Gateway         = 192.168.0.1
```

Interfaces admitidas

- 1 RACADM local
 - 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

getsvctag

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

La [tabla A-22](#) describe el subcomando `getsvctag`.

Tabla A-22. getsvctag

| Subcomando | Definición |
|------------|-----------------------------------|
| getsvctag | Muestra una etiqueta de servicio. |

Sinopsis

```
racadm getsvctag
```

Descripción

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

Ejemplo

Escriba `getsvctag` en la petición de comandos. El mensaje de salida se muestra como a continuación:

```
Y76TP0G
```

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

racdump

 **NOTA:** Para usar este comando, debe tener permiso de **Depuración**.

La [tabla A-23](#) describe el subcomando **racdump**.

Tabla A-23. racdump

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

Sinopsis

```
racadm racdump
```

Descripción

El subcomando **racdump** proporciona un solo comando para obtener el estado de un volcado e información general de la tarjeta de DRAC 5.

La información a continuación aparecerá cuando se procese el subcomando **racdump**:

- 1 Información general del sistema/RAC
- 1 Vaciado de registro de la CPU
- 1 Información de la sesión
- 1 Información del proceso
- 1 Información de la compilación del firmware

Interfaces admitidas

- 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

racreset

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

La [tabla A-24](#) describe el subcomando **racreset**.

Tabla A-24. **racreset**

| Subcomando | Definición |
|------------|-----------------------|
| racreset | Restablece el DRAC 5. |

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

Sinopsis

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

Descripción

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

Un restablecimiento forzado realiza una operación de restablecimiento del RAC. Un restablecimiento forzado debe ejecutarse únicamente como recurso de última instancia para recuperar el RAC.

 **AVISO:** Debe reiniciar el sistema después de realizar un restablecimiento forzado de DRAC 5, como se describe en la [tabla A-25](#).

La [tabla A-25](#) describe las opciones del subcomando **racreset**.

Tabla A-25. **Opciones del subcomando racreset**

| Opción | Descripción |
|--------|---|
| hard | Un restablecimiento <i>forzado</i> realiza una operación de restablecimiento a fondo en el controlador de acceso remoto. Un restablecimiento forzado se debe utilizar únicamente como recurso de última instancia para restablecer el controlador RAC a fin de recuperarlo. |
| soft | Un restablecimiento <i>ordenado</i> ejecuta una operación de reinicio ordenado del RAC. |

Ejemplos

- 1 `racadm racreset`
Inicia la secuencia de restablecimiento ordenado del DRAC 5.
- 1 `racadm racreset hard`
Inicia la secuencia de restablecimiento forzado del DRAC 5.

Interfaces admitidas

- 1 RACADM local
 - 1 RACADM remoto
 - 1 RACADM de conexión Telnet/SSH/serie
-

racresetcfg

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

La [tabla A-26](#) describe el subcomando **racresetcfg**.

Tabla A-26. racresetcfg

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

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

Descripción

El comando **racresetcfg** quita todas las anotaciones 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 el RAC y la configuración serie asignándoles los valores predeterminados originales. Después restablecimiento, el nombre predeterminado y la contraseña serán **root** y **calvin**, respectivamente, y la dirección IP será 192.168.0.120. Si se ejecuta un comando **racresetcfg** desde un cliente de red (por ejemplo, de un explorador de web admitido, Telnet/SSH o RACADM remoto), debe usar la dirección IP predeterminada.

 **NOTA:** Este subcomando también restablecerá la interfaz serie asignándole la velocidad en baudios (57600) y el puerto COM predeterminados. Es posible que la configuración de la conexión serie se tenga que reconfigurar a través de la pantalla de configuración del BIOS del servidor para poder tener acceso al RAC por medio del puerto serie.

serveraction

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

La [tabla A-27](#) describe el subcomando **serveraction**.

Tabla A-27. serveraction

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

Sinopsis

```
racadm serveraction <action>
```

Descripción

El subcomando "serveraction" permite que los usuarios realicen operaciones de administración de la alimentación en el sistema host. La [tabla A-28](#) describe las opciones de control de alimentación de **serveraction**

Tabla A-28. Opciones del subcomando serveraction

| Subcomando | Definición |
|------------|------------|
|------------|------------|

| Cadena | Definición |
|----------|--|
| <acción> | <p>Especifica la acción. Las opciones para la cadena <acción> son:</p> <ul style="list-style-type: none"> powerdown: apaga el sistema administrado. powerup: enciende el sistema administrado. powercycle: realiza una operación del ciclo de encendido en el sistema administrado. Esta acción es similar a la acción de presionar el botón de encendido en el panel anterior del sistema para apagar y luego encender el sistema. powerstatus: muestra el estado actual de alimentación del servidor ("Encendido" o "Apagado") hardreset: realiza una operación de restablecimiento (reinicio) en el sistema administrado. |

Salida

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

Interfaces admitidas

- | RACADM local
- | RACADM remoto
- | RACADM de conexión Telnet/SSH/serie

getraclog

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

La [tabla A-29](#) describe el comando `racadm`.

Tabla A-29. `getraclog`

| Comando | Definición |
|---------------------------|---|
| <code>getraclog -i</code> | Muestra el número de anotaciones en el registro del DRAC 5. |
| <code>getraclog</code> | Muestra las anotaciones del registro del DRAC 5. |

Sinopsis

```
racadm getraclog -i
```

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

Descripción

 **NOTA:** Es posible que el nombre de comando y los nombres de subcomandos `racadm` sean diferentes. Esto es normal.

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

A continuación, se muestran las opciones que permiten que el comando `getraclog` lea anotaciones:

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

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

Salida

La pantalla predeterminada del mensaje de salida muestra el número de anotación, la fecha y hora, el origen y la descripción. La marca de fecha y hora

comienza a la media noche del 1º de enero y se incrementa hasta que el sistema se inicia. Después de que el sistema se inicia, se usa la marca de 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

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

clrraclog

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

Sinopsis

```
racadm clrraclog
```

Descripción

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

getsel

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

La [tabla A-30](#) 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 cuenta] [-s cuenta] [-m]
```

Descripción

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

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

- A: especifica que el mensaje de salidas debe aparecer sin encabezados ni etiquetas.
- c: proporciona la cuenta máxima de anotaciones a generar.
- o: muestra el mensaje de salida en una sola línea.

- s: especifica la anotación inicial a partir de la cual se muestra la información
- E: coloca los 16 bytes del registro de sucesos del sistema sin procesar al final de cada línea de salida como una secuencia de valores hexadecimales.
- R: sólo se imprimen los datos sin procesar.
- m: muestra una pantalla de información a la vez y pide al usuario que continúe (es parecida al comando **more** de UNIX).

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

Salida

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

Por ejemplo:

```
Record:      1
Date/Time:  11/16/2005 22:40:43
Severity:    2
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

clrsl

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

Sinopsis

```
racadm clrsl
```

Descripción

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

gettracelog

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

La [tabla A-31](#) describe el subcomando **gettracelog**.

Tabla A-31. **gettracelog**

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

Sinopsis

```
racadm gettracelog -i
racadm gettracelog [-A] [-o] [-c cuenta] [-s anotación_de_inicio] [-m]
```

Descripción

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

- i: muestra el número de anotaciones en el registro de rastreo del DRAC 5.
- m: muestra una pantalla de información a la vez y pide al usuario que continúe (es parecida al comando **more** de UNIX).
- o: muestra el mensaje de salida en una sola línea.
- c: especifica el número de anotaciones a mostrar
- s: especifica la anotación inicial a mostrar
- A: no mostrar encabezados ni etiquetas

Salida

La pantalla predeterminada del mensaje de salida muestra el número de anotación, la fecha y hora, el origen y la descripción. La marca de fecha y hora comienza a la media noche del 1º de enero y se incrementa hasta que el sistema se inicia. Después de que el sistema se inicia, se usa la marca de fecha y hora del sistema.

Por ejemplo:

```
Record: 1
Date/Time: Dec 8 08:21:30
Source: ssmgrd[175]
Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

sslcsrgen

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

La [tabla A-32](#) describe el subcomando **sslcsrgen**.

Tabla A-32. sslcsrgen

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

Sinopsis

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

Descripción

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

Opciones

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

La [tabla A-33](#) describe las opciones del subcomando **sslcsrgen**.

Tabla A-33. Opciones del subcomando sslcsrgen

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

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

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

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

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

Restricciones

El subcomando **sslcsrgen** sólo se puede ejecutar desde un cliente RACADM local o remoto y no se puede usar en las interfaces serie, Telnet o SSH.

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

Ejemplos

```
racadm sslcsrgen -s
```

```
o
```

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

sslcertupload

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

La [tabla A-34](#) describe el subcomando **sslcertupload**.

Tabla A-34. sslcertupload

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

Sinopsis

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

Opciones

La [tabla A-35](#) describe las opciones del subcomando **sslcertupload**.

Tabla A-35. Opciones del subcomando **sslcertupload**

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

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

Restricciones

El subcomando **sslcertupload** sólo se puede ejecutar desde un cliente RACADM local o remoto. El subcomando **sslsrgrn** no se puede usar en las interfaces serie, Telnet o SSH.

Ejemplo

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

Interfaces admitidas

- I RACADM local
- I RACADM remoto

sslcertdownload

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

La [tabla A-36](#) 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

La [tabla A-37](#) describe las opciones del subcomando **sslcertdownload**.

Tabla A-37. Opciones del subcomando **sslcertdownload**

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

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

Restricciones

El subcomando **sslcertdownload** sólo se puede ejecutar desde un cliente RACADM local o remoto. El subcomando **sslcsrgen** no se puede usar en las interfaces serie, Telnet o SSH.

Ejemplo

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto

sslcertview

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

La [tabla A-38](#) describe el subcomando **sslcertview**.

Tabla A-38. sslcertview

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

Sinopsis

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

Opciones

La [tabla A-39](#) describe las opciones del subcomando **sslcertview**

Tabla A-39. Opciones del subcomando sslcertview

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

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1

Serial Number          : 00

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

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
Certificado predeterminado de DRAC5
US
Texas
Round Rock
Dell Inc.
Remote Access Group
Certificado predeterminado de DRAC5
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

testemail

La [tabla A-40](#) describe el subcomando **testemail**.

Tabla A-40. Configuración de testemail

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

Sinopsis

```
racadm testemail -i <index>
```

Descripción

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

Antes de ejecutar el comando "testemail", asegúrese que el índice especificado en el grupo [cfgEmailAlert](#) de RACADM esté activado y configurado correctamente. La [tabla A-41](#) muestra una lista y los comandos asociados del grupo [cfgEmailAlert](#).

Tabla A-41. Configuración de testemail

| Acción | Comando |
|--|---|
| Activar la alerta | racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1 |
| Establecer la dirección de correo electrónico de destino | racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com |
| Establecer 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!" |
| Comprobar que la dirección IP de SNMP está correctamente configurada | racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr -i 192.168.0.152 |
| Ver los valores actuales de alerta de correo electrónico | racadm getconfig -g cfgEmailAlert -i <índice> donde <índice> es un número de 1 a 4 |

Opciones

La [tabla A-42](#) describe las opciones del subcomando **testemail**

Tabla A-42. Subcomandos de testemail

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

Salida

Ninguna.

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

testtrap

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

La [tabla A-43](#) describe el subcomando **testtrap**.

Tabla A-43. testtrap

| Subcomando | Descripción |
|------------|--|
| testtrap | Prueba la función de alertas de capturas 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 receptor de capturas de destino especificado en la red.

Antes ejecutar el comando "testtrap", asegúrese que el índice especificado en el grupo [cfgIpmiPet](#) de RACADM está configurado correctamente.

La [tabla A-41](#) muestra una lista y los comandos asociados del grupo [cfgIpmiPet](#).

Tabla A-44. Comandos cfgEmailAlert

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

Entrada

La [tabla A-45](#) describe las opciones del subcomando **testtrap**

Tabla A-45. Opciones del subcomando testtrap

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

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

vmdisconnect

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

La [tabla A-46](#) describe el subcomando **vmdisconnect**.

Tabla A-46. vmdisconnect

| Subcomando | Descripción |
|--------------|---|
| vmdisconnect | Cierra todas las conexiones de medios virtuales de RAC de los clientes remotos. |

Sinopsis

```
racadm vmdisconnect
```

Descripción

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

El subcomando **vmdisconnect** habilita a un usuario del RAC para que desconecte todas las sesiones de medios virtuales activas. Las sesiones de medios virtuales activas se pueden mostrar en la interfaz gráfica de usuario del RAC o por medio del subcomando [getsysinfo](#) de racadm.

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

vmkey

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

La [tabla A-47](#) describe el subcomando **vmkey**.

Tabla A-47. vmkey

| Subcomando | Descripción |
|------------|--|
| vmkey | Realiza operaciones relacionadas con la clave de medios virtuales. |

Sinopsis

```
racadm vmkey <acción>
```

Si la <acción> se establece como `reset`, la memoria flash virtual se restablecerá y tomará el tamaño predeterminado de 16 MB.

Descripción

Cuando una imagen de clave de medios virtuales personalizada se carga en el RAC, el tamaño de la clave se convierte en el tamaño de la imagen. El subcomando "vmkey" se puede usar para restablecer la clave asignándole el tamaño predeterminado original, que es de 16 MB en el DRAC 5.

Interfaces admitidas

- 1 RACADM local
- 1 RACADM remoto
- 1 RACADM de conexión Telnet/SSH/serie

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Definiciones de grupos y objetos de la base de datos de propiedades de DRAC 5

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Caracteres que se pueden mostrar](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgNetTuning](#)
- [cfgOobSnmpp](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgIpmiSerial](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen los siguientes:

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

idRacInfo

Este grupo contiene parámetros de la pantalla para proporcionar información acerca de las características específicas del DRAC 5 al 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 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 los servidores Dell PowerEdge."

Descripción

Una descripción de texto del tipo de RAC.

idRacVersionInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

"1.0"

Descripción

Cadena que contiene la versión actual del firmware del producto.

idRacBuildInfo (sólo lectura)

Valores legales

Cadena de hasta 16 caracteres ASCII.

Predeterminado

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

Descripción

Cadena que contiene la versión de compilación del producto actual.

idRacName (sólo lectura)

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

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 DRAC 5.

cfgLanNetworking

Este grupo contiene parámetros para configurar el NIC del DRAC 5.

Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca el NIC del DRAC 5, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP del NIC 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgDNSDomainName (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted 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. Los caracteres permitidos son los alfanuméricos, '-' (guión) y '.' (punto).

 **NOTA:** Microsoft® Active Directory® sólo admite nombres de dominio totalmente calificados (FQDN) de 64 bytes o menos.

Predeterminado

""

Descripción

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

cfgDNSRacName (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted 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 servidores DNS sólo registran nombres de 31 caracteres o menos.

Predeterminado

rac-etiqueta de servicio

Descripción

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

cfgDNSRegisterRac (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Registra el nombre del DRAC 5 en el servidor DNS.

cfgDNSServersFromDHCP (Lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgDNSServer1 (Lectura/escritura)

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

Valores legales

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

Descripción

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

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

cfgDNSServer2 (Lectura/escritura)

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

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

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

cfgNicEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgNicIpAddress (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted debe tener permiso para **Configurar el DRAC 5**. Este parámetro es configurable sólo si el parámetro `cfgNicUseDhcp` se establece en **0** (FALSO).

Valores legales

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

Predeterminado

192.168.0.120

Descripción

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

cfgNicNetmask (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted debe tener permiso para **Configurar el DRAC 5**. Este parámetro es configurable sólo si el parámetro **cfgNicUseDhcp** se establece en **0** (FALSO).

Valores legales

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

Predeterminado

255.255.255.0

Descripción

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

cfgNicGateway (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted debe tener permiso para **Configurar el DRAC 5**. Este parámetro es configurable sólo si el parámetro **cfgNicUseDhcp** se establece en **0** (FALSO).

Valores legales

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

Predeterminado

192.168.0.1

Descripción

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

cfgNicUseDhcp (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

 **NOTA:** Si actualiza el sistema de manera remota, utilice el comando [setniccfg](#).

cfgNicSelection (lectura/escritura)

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

Valores legales

0 (compartido)

1 (compartido con protección contra fallas)

2 (dedicado)

Predeterminado

2

Descripción

Especifica el modo actual de operación para el controlador de interfaces 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 el NIC integrado del servidor host se comparte con el RAC en el servidor host. Este modo permite que las configuraciones utilicen la misma dirección IP en el servidor host y el RAC para tener accesibilidad común en la red. |
| Compartido con protección contra fallas | Habilita la capacidad de modo colaborativo entre los controladores de interfaces de red integrados del servidor host. |
| Dedicado | Especifica que el NIC del RAC se debe usar como NIC dedicado para la accesibilidad remota. |

cfgNicMacAddress (sólo lectura)

Valores legales

Una cadena que represente la dirección MAC del NIC del RAC.

Predeterminado

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

Descripción

La dirección MAC del NIC del RAC.

cfgNicVlanEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgNicVlanId (lectura/escritura)

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

Valores legales

0 – 4094

Predeterminado

0

Descripción

Especifica la identificación de VLAN para la configuración de red VLAN. Esta propiedad es válida sólo si `cfgNicVlanEnable` se establece en **1** (activado).

cfgNicVlanPriority (lectura/escritura)

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

Valores legales

0 – 7

Predeterminado

0

Descripción

Especifica la prioridad de VLAN para la configuración de red VLAN. Esta propiedad es válida sólo si `cfgNicVlanEnable` se establece en **1** (activado).

cfgRemoteHosts

Este grupo proporciona propiedades que permiten la configuración de varios componentes remotos, que incluyen al servidor SMTP para alertas por correo electrónico y a las direcciones IP del servidor TFTP para actualizaciones de firmware.

cfgRhostsSmtServerIpAddr (lectura/escritura)

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

Valores legales

Una cadena que represente una dirección IP válida de servidor de SMTP. Por ejemplo, 192.168.0.55.

Predeterminado

0.0.0.0

Descripción

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

cfgRhostsFwUpdateTftpEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

Activa o desactiva la actualización de firmware del RAC desde una servidor TFTP de red.

cfgRhostsFwUpdateIpAddr (lectura/escritura)

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

Valores legales

Una cadena que represente 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 realizar las operaciones de actualización del firmware del RAC por TFTP.

cfgRhostsFwUpdatePath (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 255.

Predeterminado

...

Descripción

Especifica la ruta de acceso de TFTP en la que se encuentra el archivo de imagen del firmware del RAC, en el servidor TFTP. La ruta de acceso de TFTP está en relación a la ruta raíz de TFTP en el servidor TFTP.

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

cfgUserAdmin

Este grupo proporciona la información de configuración acerca de los usuarios que tienen permiso de acceder al RAC por medio de las interfaces remotas disponibles.

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

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted 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, usted 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 serie de IPMI.

cfgUserAdminPrivilege (Lectura/escritura)

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

Valores legales

De 0x0000000 a 0x00001ff, y 0x0

Predeterminado

0x0000000

Descripción

Esta propiedad especifica los privilegios de autoridad basada en funciones que se otorgan al usuario. El valor se representa como máscara de bits que permite definir cualquier combinación de valores de privilegios. La [tabla B-2](#) describe las máscaras de bits de los privilegios de usuario permitidos.

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

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

Ejemplos

La [tabla B-3](#) proporciona ejemplos de las máscaras de bits de privilegios para usuarios con uno o varios privilegios.

Tabla B-3. Ejemplos de máscaras de bit para privilegios del usuario

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

cfgUserAdminUserName (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 16.

Predeterminado

""

Descripción

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

 **NOTA:** Este valor de propiedad DEBE ser único y distinto de otras instancias de usuarios.

cfgUserAdminPassword (de sólo escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva a un usuario individual.

cfgUserAdminSolEnable

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgEmailAlert

Este grupo contiene parámetros para configurar la capacidad de alertas por correo electrónico del RAC.

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

cfgEmailAlertIndex (sólo lectura)

Valores legales

1-4

Predeterminado

Este parámetro se llena en base a las instancias existentes.

Descripción

El índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Especifica la dirección de correo electrónico de destino para las alertas por correo electrónico. Por ejemplo, `user1@company.com`.

cfgEmailAlertAddress (sólo lectura)

Valores legales

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

Predeterminado

...

Descripción

La dirección de correo electrónico de la fuente de alerta.

cfgEmailAlertCustomMsg (sólo lectura)

Valores legales

Cadena. Número máximo de caracteres = 32.

Predeterminado

""

Descripción

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

cfgSessionManagement

Este grupo contiene parámetros para configurar el número de sesiones que se pueden conectar al 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 - 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

10 -1920

Predeterminado

30

Descripción

Define el tiempo de espera sin actividad, expresado en segundos, para la interfaz de RACADM remoto. Si una sesión RACADM remota permanece inactiva durante más tiempo del que se especifica para las sesiones, la sesión se cerrará.

cfgSsnMgtWebserverTimeout (lectura/escritura)

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

Valores legales

60 – 1920

Predeterminado

300

Descripción

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

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

cfgSsnMgtSshIdleTimeout (lectura/escritura)

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

Valores legales

0 (Sin expiración de tiempo)

60 – 1920

Predeterminado

300

Descripción

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

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

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

(Advertencia: La sesión ya no es válida, es posible que haya agotado el tiempo de espera)

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

cfgSsnMgtTelnetTimeout (lectura/escritura)

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

Valores legales

0 (Sin expiración de tiempo)

Predeterminado

0

Descripción

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

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

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

(Advertencia: La sesión ya no es válida, es posible que haya agotado el tiempo de espera)

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

cfgSerial

Este grupo contiene parámetros de configuración 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, usted 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de consola serie del RAC.

cfgSerialConsoleQuitKey (lectura/escritura)

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

Valores legales

CADENA

MaxLen = 4

Predeterminado

^\
(<Ctrl><\>)

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

Descripción

Esta tecla, o combinación de teclas, finaliza la redirección de consola de texto cuando se usa el comando `connect com2`. El valor de `cfgSerialConsoleQuitKey` se puede representar con uno de los siguientes valores:

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

cfgSerialConsoleIdleTimeout (lectura/escritura)

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

Valores legales

0 = ningún tiempo de espera

60 – 1920

Predeterminado

300

Descripción

El número máximo de segundos a esperar antes de desconectar una sesión serie sin actividad.

cfgSerialConsoleNoAuth (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted 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 de inicio de sesión de la consola serie del RAC.

cfgSerialConsoleCommand (lectura/escritura)

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

Descripción

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

Predeterminado

""

Ejemplo

"connect com2"

cfgSerialHistorySize (lectura/escritura)

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

Valores legales

0 – 8192

Predeterminado

8192

Descripción

Especifica el tamaño máximo del búfer de historial serie.

cfgSerialSshEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgSerialTelnetEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgSerialCom2RedirEnable (lectura/escritura)

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

Predeterminado

1

Valores legales

1 (VERDADERO)

0 (FALSO)

Descripción

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

cfgNetTuning

Este grupo permite a los usuarios configurar los parámetros avanzados de la interfaz de red para el NIC del RAC. Cuando se configura, los valores actualizados pueden tardar hasta un minuto en activarse.

 **AVISO:** Tenga precaución especial al modificar las propiedades en este grupo. La modificación inadecuada de las propiedades en este grupo puede hacer que el NIC del RAC no pueda funcionar.

cfgNetTuningNicAutoneg (Lectura/escritura)

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

Valores legales

1 (activado)

0 (desactivado)

Predeterminado

1

Descripción

Activa la negociación automática del modo dúplex y la velocidad de 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 (10 Mbits)

1 (100 Mbits)

Predeterminado

1

Descripción

Especifica la velocidad de uso del NIC del RAC. Esta propiedad no se utiliza cuando `cfgNetTuningNicAutoNeg` está establecido en **1** (activado).

cfgNetTuningNicFullDuplex (Lectura/escritura)

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

Valores legales

0 (semidúplex)

1 (dúplex total)

Predeterminado

1

Descripción

Especifica la configuración de dúplex del NIC del RAC. Esta propiedad no se utiliza cuando `cfgNetTuningNicAutoNeg` está establecido en **1** (activado).

cfgNetTuningNicMtu (lectura/escritura)

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

Valores legales

576 - 1500

Predeterminado

1500

Descripción

El tamaño en bytes de la unidad de transmisión máxima usada por el NIC del DRAC 5.

cfgNetTuningTcpSrttDflt (lectura/escritura)

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

Valores legales

6 - 384

Predeterminado

6

Descripción

El valor predeterminado base sin irregularidades del tiempo de espera de la trayectoria de ida y vuelta para el tiempo de ida y vuelta de retransmisión de TCP expresado en unidades de medio segundo. (Escriba valores hexadecimales.)

cfgOobSntp

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.

cfgOobSntpAgentCommunity (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 31.

Predeterminado

público

Descripción

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

cfgOobSntpAgentEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Activa o desactiva al agente SNMP en el RAC.

cfgRacTuning

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

cfgRacTuneHttpPort (Lectura/escritura)

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

Valores legales

10 – 65535

Predeterminado

80

Descripción

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

cfgRacTuneHttpsPort (Lectura/escritura)

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

Valores legales

10 – 65535

Predeterminado

443

Descripción

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

cfgRacTuneIpRangeEnable

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgRacTunel pRangeAddr

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

Valores legales

Cadena en formato de dirección IP. Por ejemplo, 192.168.0.44.

Predeterminado

192.168.1.1

Descripción

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

cfgRacTunel pRangeMask

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

Valores legales

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

Predeterminado

255.255.255.0

Descripción

Cadena en formato de dirección IP. Por ejemplo, 255.255.255.0.

cfgRacTunel pBIkEnable

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgRacTuneIpBlkFailcount

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

Valores legales

2 - 16

Predeterminado

5

Descripción

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

cfgRacTuneIpBlkFailWindow

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

Valores legales

2 - 65535

Predeterminado

60

Descripción

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

cfgRacTuneIpBlkPenaltyTime

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

Valores legales

2 - 65535

Predeterminado

300

Descripción

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

cfgRacTuneSshPort (lectura/escritura)

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

Valores legales

1 – 65535

Predeterminado

22

Descripción

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

cfgRacTuneTelnetPort (Lectura/escritura)

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

Valores legales

1 – 65535

Predeterminado

23

Descripción

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

cfgRacTuneRemoteRacadmEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

1

Descripción

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

cfgRacTuneConRedirEncryptEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Cifra la codificación de vídeo en una sesión de redirección de consola.

cfgRacTuneConRedirPort (Lectura/escritura)

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

Valores legales

1 – 65535

Predeterminado

5901

Descripción

Especifica el puerto que se debe usar para tráfico 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 – 65535

Predeterminado

5901

Descripción

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

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

cfgRacTuneAsrEnable (lectura/escritura)

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

Valores legales

1 – 65535

Predeterminado

5901

Descripción

Activa o desactiva la función de captura de pantallas 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

0 – 60

Predeterminado

0

Descripción

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

cfgRacTuneTimezoneOffset (lectura/escritura)

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

Valores legales

-720 – 780

Predeterminado

0

Descripción

Especifica la compensación zona horaria (en minutos) con respecto a la hora GMT/UTC que se debe usar para la hora del RAC. A continuación, se muestran algunas compensaciones comunes para las zonas horarias en los Estados Unidos:

-480 (PST: horario de la costa oeste)

-420 (MST: horario de las Montañas Rocosas)

-360 (CST: horario del centro)

-300 (EST: horario de la costa este)

cfgRacTuneWebserverEnable (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

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 clientes ni por RACADM remoto. Esta propiedad no tiene ningún efecto en las interfaces Telnet, SSH, serie o RACADM local.

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 255.

Predeterminado

""

Descripción

El nombre del host del sistema administrado.

ifcRacMnOsOsName (lectura/escritura)

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

Valores legales

Cadena. Número máximo 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 en este grupo SE DEBEN configurar antes de generar una CSR del RAC.

Consulte los detalles del subcomando [sslcsrgen](#) de RACADM para obtener más información acerca de la generación de solicitudes de firma de certificados.

cfgSecCsrCommonName (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica el nombre común (CN) de la CSR.

cfgSecCsrOrganizationName (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrOrganizationUnit (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrLocalityName (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica la localidad (L) de la CSR.

cfgSecCsrStateName (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

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

cfgSecCsrCountryCode (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 2.

Predeterminado

""

Descripción

Especifica el código del país (CC) de la CSR

cfgSecCsrEmailAddr (lectura/escritura)

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

Valores legales

Cadena. Número máximo de caracteres = 254.

Predeterminado

""

Descripción

Especifica la dirección de correo electrónico de CSR.

cfgSecCsrKeySize (lectura/escritura)

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

Valores legales

512

1024

2048

Predeterminado

1024

Descripción

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

cfgRacVirtual

Este grupo contiene parámetros para configurar la característica 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, usted debe tener permiso para **Configurar el DRAC 5**.

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

Este objeto se usa para conectar los dispositivos virtuales al sistema por medio del bus USB. Cuando los dispositivos se conecten, el servidor reconocerá los dispositivos USB de almacenamiento masivo que estén conectados al sistema. Esto equivale a conectar un CD-ROM USB local, o unidad de disquete, a un puerto USB del sistema. Cuando los dispositivos estén conectados, usted podrá conectarse a los dispositivos virtuales de manera remota por medio de la interfaz gráfica de usuario del DRAC5 o de la CLI. Si establece un valor de 0 para este objeto, hará que los dispositivos se desconecten del bus USB.

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

cfgVirAtapiSrvPort (Lectura/escritura)

 **NOTA:** Para modificar esta propiedad, se debe tener permiso para **Acceder a los medios virtuales**.

Valores legales

1 - 65535

Predeterminado

3669

Descripción

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

cfgVirAtapiSrvPortSsl (lectura/escritura)

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

Valores legales

Cualquier número de puerto no utilizado entre 0 y 65535 en decimales.

Predeterminado

3669

Descripción

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

cfgVirMediaKeyEnable (lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgVirMediaBootOnce (lectura/escritura)

 **NOTA:** Para modificar esta propiedad, usted 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 a partir de los medios virtuales del RAC. Si esta propiedad está activada cuando el servidor host se reinicia, la función intentará iniciar a partir de los dispositivos de medios virtuales; si los medios adecuados están instalados en el dispositivo.

cfgActiveDirectory

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

cfgADracDomain (Lectura/escritura)

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

Valores legales

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

Predeterminado

""

Descripción

El dominio de Active Directory en que reside el DRAC.

cfgADracName (Lectura/escritura)

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

Valores legales

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

Predeterminado

""

Descripción

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

cfgADEnable (Lectura/escritura)

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

Valores legales

1 (VERDADERO)

0 (FALSO)

Predeterminado

0

Descripción

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

cfgADAuthTimeout (Lectura/escritura)

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

Valores legales

15 – 300

Predeterminado

120

Descripción

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

cfgADRootDomain, (lectura/escritura)

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

Valores legales

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

Predeterminado

""

Descripción

Dominio raíz del bosque del dominio.

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, usted 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 en 0 (desactivado), el puerto serie del DRAC 5 se convierte en el puerto serie de IPMI. Esta propiedad determina el modo del puerto serie definido por IPMI.

En el modo básico, el puerto utiliza datos binarios para comunicarse con un programa de aplicación en el cliente serie. En el modo de terminal, el puerto supone que hay una terminal ASCII sin procesador conectada y permite introducir comandos muy simples.

cfgIpmiSerialBaudRate (lectura/escritura)

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

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

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

cfgIpmiSerialChanPrivLimit (lectura/escritura)

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

Valores legales

0 (Ninguna)

1 (CTS/RTS)

2 (XON/XOFF)

Predeterminado

1

Descripción

Especifica el valor del control de flujo para el puerto serie de IPMI.

cfgIpmiSerialHandshakeControl (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialLineEdit (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialEchoControl (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSerialDeleteControl (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

0

Descripción

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

cfgIpmiSerialNewLineSequence (lectura/escritura)

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

Valores legales

0 (Ninguna)

1 (retorno de carro, salto de línea)

2 (NULO)

3 (<retorno de carro>)

4 (<salto de línea, retorno de carro>)

5 (<salto de línea>)

Predeterminado

1

Descripción

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

cfgIpmiSerialInputNewLineSequence (lectura/escritura)

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

Valores legales

0 (<ENTRAR>)

1 (NULO)

Predeterminado

1

Descripción

Indica la especificación de la secuencia para introducción de nueva línea en la interfaz serie de IPMI.

cfgIpmiSol

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

cfgIpmiSolEnable (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

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

cfgIpmiSolBaudRate (lectura/escritura)

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

Valores legales

9600, 19200, 57600, 115200

Predeterminado

57600

Descripción

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

cfgIpmiSolMinPrivilege (lectura/escritura)

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

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSolAccumulateInterval (lectura/escritura)

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

Valores legales

1 – 255.

Predeterminado

10

Descripción

Especifica la cantidad típica de tiempo que el BMC espera antes de transmitir un paquete parcial de datos de caracteres de comunicación en serie en la LAN. Este valor se basa en incrementos de 5 ms a partir de 1.

cfgIpmiSolSendThreshold (lectura/escritura)

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

Valores legales

1 – 255

Predeterminado

255

Descripción

El valor límite del umbral de la SOL.

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de IPMI en la LAN.

cfgIpmiLanPrivLimit (lectura/escritura)

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

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

0

Descripción

Especifica el nivel máximo de privilegios que se requiere para tener acceso a la IPMI en la LAN.

cfgIpmiLanAlertEnable (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva el envío global de alertas por correo electrónico. Esta propiedad suprime todas las propiedades de activación y desactivación del envío de alertas individuales por correo electrónico.

cfgIpmiEncryptionKey (lectura/escritura)

 **NOTA:** Para ver o modificar esta propiedad, usted 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, usted 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 usa para configurar los filtros de sucesos de plataforma que están disponibles en el servidor administrado.

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

cfgIpmiPefName (sólo lectura)

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

Valores legales

Cadena. Número máximo de caracteres = 255.

Predeterminado

El nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de sucesos de plataforma.

cfgIpmiPefIndex (sólo lectura)

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

Valores legales

Predeterminado

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

Descripción

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

cfgIpmiPefAction (lectura/escritura)

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

Valores legales

- 0 (Ninguna)
- 1 (Apagar)
- 2 (Restablecer)
- 3 (Ciclo de encendido)

Predeterminado

0

Descripción

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

cfgIpmiPefEnable (lectura/escritura)

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

Valores legales

- 0 (FALSO)
- 1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva un filtro específico de sucesos de plataforma.

cfgIpmiPet

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

cfgIpmiPetIndex (lectura/escritura)

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

Valores legales

1 - 4

Predeterminado

El valor de índice adecuado.

Descripción

Identificador único del índice que corresponde a la captura.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

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

Valores legales

0 (FALSO)

1 (VERDADERO)

Predeterminado

1

Descripción

Activa o desactiva una captura específica.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Interfaces de RACADM admitidas

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

La tabla a continuación proporciona una descripción de los subcomandos RACADM y la compatibilidad de los mismos con la interfaz correspondiente.

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

| Subcomando | Telnet/SSH/serie | RACADM local | RACADM remoto |
|-----------------|------------------|--------------|---------------|
| 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 | ✗ | ✓ | ✓ |
| testemail | ✓ | ✓ | ✓ |
| testtrap | ✓ | ✓ | ✓ |
| vmdisconnect | ✓ | ✓ | ✓ |
| vmkey | ✓ | ✓ | ✓ |

✓ = Compatible; ✗ = No compatible

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Descripción de DRAC 5

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Lo nuevo en esta versión de DRAC 5](#)
- [Características del hardware del DRAC 5](#)
- [Especificaciones de hardware](#)
- [Conexiones de acceso remoto admitidas](#)
- [Características de seguridad del DRAC 5](#)
- [Plataformas admitidas](#)
- [Sistemas operativos admitidos](#)
- [Exploradores de web admitidos](#)
- [Características](#)
- [Otros documentos que puede necesitar](#)

El Dell™ Remote Access Controller 5 (DRAC 5) es un hardware de administración de sistemas y una solución de software diseñada para proporcionar capacidades de administración remotas, recuperación de sistemas bloqueados y funciones de control de alimentación para sistemas Dell PowerEdge™.

Al comunicarse con el controlador de administración de la placa base (BMC) del sistema, el DRAC 5 (cuando se tiene instalado) se puede configurar para enviarle alertas por correo electrónico para advertencias o errores relacionados con voltajes, temperaturas, intromisiones y velocidades de ventilador. El DRAC 5 también registra datos de sucesos y la pantalla de bloqueo más reciente (sólo para sistemas que ejecutan el sistema operativo Microsoft® Windows®) para ayudarle a diagnosticar la causa probable de un bloqueo del sistema.

El DRAC 5 tiene su propio microprocesador y memoria y recibe alimentación del sistema en el que está instalado. El DRAC 5 se puede preinstalar en su sistema o está disponible de forma independiente en un paquete.

Para iniciarse con el DRAC 5, consulte "[Instalación y configuración del DRAC 5](#)".

Lo nuevo en esta versión de DRAC 5

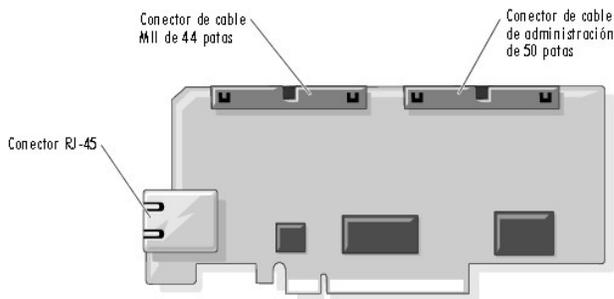
En este producto, la versión 1.0 del firmware de DRAC 5 es compatible con lo siguiente:

- 1 Bloqueo y filtración de direcciones IP. Consulte "[Habilitación de las opciones de seguridad adicionales del DRAC 5](#)".
- 1 Interfaz de Protocolo de línea de comandos para administración de servidor (SM-CLP) del Grupo de trabajo de administración de servidor (SMWG). Consulte "[Uso de la interfaz de línea de comandos de SM-CLP del DRAC 5](#)".
- 1 Configuración de los desencadenadores y filtros de sucesos de plataforma. Consulte "[Configuración de sucesos de plataforma](#)".
- 1 Configuración y consulta de la información de sensores.
- 1 Compatibilidad con IPMI 2.0
- 1 Compatibilidad con medios USB.

Características del hardware del DRAC 5

La [figura 1-1](#) muestra el hardware del DRAC 5.

Figura 1-1. Características del hardware del DRAC 5



Especificaciones de hardware

Requisitos de alimentación

La [tabla 1-1](#) muestra una lista de los requisitos de alimentación del DRAC 5.

Tabla 1-1. Requisitos de alimentación del DRAC 5

Alimentación del sistema

| |
|--|
| 1,2 A en la toma auxiliar de +3,3 V (máximo) |
| 550 mA en la toma principal de +3,3 V (máximo) |
| 0 mA en la toma principal de +5 V (máximo) |

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 controlador de interfaces de red incorporado en la tarjeta, de 10/100 Mbps y conector RJ-45, un cable de administración de 50 patas y un cable MII de 44 patas. Consulte la [figura 1-1](#) para ver los conectores de cables del DRAC 5.

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

Con los cables de administración y MII, usted puede configurar el DRAC en tres modos distintos, según sus necesidades. Para obtener más información, consulte "[Modos del DRAC](#)" en la sección "[Uso de la interfaz de línea de comandos de RACADM](#)".

Puertos del DRAC 5

La [tabla 1-2](#) identifica los puertos en los que el DRAC 5 busca una conexión de servidor. La [tabla 1-3](#) identifica los puertos que el DRAC 5 utiliza como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un 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 de SNMP |
| 443* | HTTPS |
| 623 | RMCP/RMCP+ |
| 3668* | Servidor de medios virtuales |
| 3669* | Servicio de medios virtuales seguros |
| 5900* | Redirección de teclado y mouse de consola |
| 5901* | Redirección de vídeo 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 en DHCP |
| 69 | TFTP |
| 162 | captura SNMP |
| 636 | LDAPS |
| 3269 | LDAPS para catálogo global (GC) |

Conexiones de acceso remoto admitidas

La [tabla 1-4](#) lista las características de las conexiones.

Tabla 1-4. Conexiones de acceso remoto admitidas

| | |
|--|--|
| | |
|--|--|

| Conexión | Características |
|----------------|---|
| NIC del DRAC 5 | <ul style="list-style-type: none"> 1 Ethernet 10/100 Mbps 1 Compatibilidad con DHCP 1 Notificación de sucesos de capturas SNMP y de correo electrónico 1 Interfaz de red dedicada para la interfaz basada en web del DRAC 5 1 Compatibilidad para la consola Telnet/SSH y los comandos de CLI de RACADM incluyendo los comandos de inicio, restablecimiento, encendido y apagado del sistema |
| Puerto serie | <ul style="list-style-type: none"> 1 Compatibilidad para la consola serie y los comandos de CLI de RACADM incluyendo los comandos de inicio, restablecimiento, encendido y apagado del sistema 1 Compatibilidad para la redirección de consola de sólo texto para un emulador de terminal o terminal VT-100 |

Características de seguridad del DRAC 5

El DRAC 5 proporciona las características de seguridad siguientes:

- 1 Autenticación de usuarios por medio de Microsoft® Active Directory® (opcional) o mediante contraseñas e identificaciones de usuario almacenadas en el hardware
- 1 Autoridad basada en funciones, lo que hace posible que cada usuario se configure con privilegios específicos
- 1 Configuración de contraseñas e identificaciones de usuario mediante la interfaz basada en web o la CLI de RACADM
- 1 El funcionamiento de la CLI de RACADM y la interfaz basada en web, que admite el cifrado SSL de 128 bits y 40 bits (para países donde no se admite el de 128 bits)

 **NOTA:** Telnet no admite la codificación de SSL.

- 1 Configuración de tiempo de espera de sesión (en segundos) mediante la interfaz basada en web o CLI de RACADM
- 1 Puertos de IP configurables (cuando sea aplicable)
- 1 Secure Shell (SSH), que utiliza una capa de transporte cifrado para tener una mayor seguridad.
- 1 Límites de fallas de inicio de sesión por cada dirección IP, con bloqueo dirección IP para inicio de sesión cuando la misma exceda el límite.
- 1 Rango de direcciones IP limitado para clientes que se conecten al DRAC 5

Plataformas admitidas

El DRAC 5 es compatible con los siguientes sistemas PowerEdge:

- 1 1900
- 1 1950
- 1 2900
- 1 2950

Consulte la *Guía de compatibilidad de Dell PowerEdge* que se encuentra en el sitio web de asistencia Dell Support en support.dell.com para conocer las plataformas compatibles más recientes.

Sistemas operativos admitidos

La [tabla 1-5](#) muestra una lista de los sistemas operativos que son compatibles con el DRAC 5.

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

Tabla 1-5. Sistemas operativos admitidos

| Familia de sistemas operativos | Sistema operativo |
|--------------------------------|---|
| Microsoft | <ul style="list-style-type: none"> Windows® 2000 Server con Service Pack 4 (SP4) Windows Server™ 2003 ediciones Standard y Enterprise con Service Pack 1 (SP1) Windows Server 2003 ediciones Standard y Enterprise R2 Windows Server 2003 ediciones Standard y Enterprise x64 Windows Storage Server 2003 R2 ediciones x64 |
| Red Hat® Linux | Enterprise Linux AS, ES y WS (versión 3) para Intel x86 y la tecnología Intel® de memoria extendida 64 (Intel EM64T) |

| | |
|-------------|--|
| | Enterprise Linux AS, ES y WS (versión 4) para Intel x86 y la tecnología Intel® de memoria extendida 64 (Intel EM64T) |
| SUSE® Linux | Enterprise Server (versión 9) with actualización 3 para Intel EM64T |

Exploradores de web admitidos

 **NOTA:** Las opciones de redirección de consola y de medios virtuales son compatibles únicamente con los exploradores de web de 32 bits. El uso de exploradores de web de 64 bits puede producir resultados inesperados.

La [tabla 1-6](#) muestra una lista de los exploradores de web que son compatibles con el DRAC 5.

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

Tabla 1-6. Exploradores de web admitidos

| Sistema operativo | Explorador web compatible |
|-------------------|---|
| Microsoft Windows | <p>Internet Explorer 6.0 (de 32 bits) con Service Pack 1 (SP1) o posterior.</p> <p>Para ver las versiones traducidas de la interfaz basada en web del DRAC 5:</p> <ol style="list-style-type: none"> 1. Abra el Panel de control de Windows. 2. Haga doble clic en el icono Configuración regional. 3. Seleccione la opción local deseada en el menú desplegable Su idioma (ubicación). <p>AVISO: Si está ejecutando el cliente de Medios virtuales, deberá usar Internet Explorer 6.0 con Service Pack 1 o posterior.</p> |
| Linux | <p>Mozilla 1.7.8 o posterior (de 32 bits).</p> <p>Mozilla Firefox 1.0.7 o posterior (de 32 bits).</p> |

Desactivación de la función de lista blanca de sitios permitidos en Mozilla Firefox

Firefox incluye una "lista blanca" de sitios permitidos que proporciona seguridad adicional. Cuando se activa la función de "lista blanca" de sitios permitidos, el explorador solicita permiso del usuario para instalar los complementos de cada uno de los sitios que ofrecen el complemento. Este proceso requiere que usted instale un complemento para cada IP/nombre_DNS de RAC, aun cuando las versiones del complemento sean idénticas.

Para desactivar la función de lista blanca de sitios permitidos y evitar las instalaciones repetitivas e innecesarias de complementos, realice los pasos a continuación:

1. Abra una ventana del explorador de web Firefox.
2. En el campo de dirección, escriba lo siguiente y presione <Entrar>:
`about:config`
3. En la columna **Nombre de la preferencia**, localice **xpinstall.whitelist.required** y haga clic en el mismo.

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

Asegúrese que **Valor** esté definido como **true**. Si no es así, haga doble clic en **xpinstall.enabled** para establecer **Valor** como **true**.

Características

El DRAC 5 ofrece las funciones siguientes:

- 1 Registro de sistema de nombres de dominio (DNS) dinámico
- 1 Administración remota y supervisión de sistemas mediante interfaz basada en web, conexión en serie o conexión Telnet.
- 1 Compatibilidad para autenticación de Active Directory: centraliza todas las identificaciones y contraseñas de usuarios del DRAC 5 en Active Directory a través de esquema de complemento opcional de Dell.
- 1 Redirección de consola: ofrece funciones de teclado, vídeo y mouse del sistema remoto.
- 1 Medios virtuales: permiten que un sistema administrado pueda acceder a una unidad de medios en la estación de administración.

- 1 Acceso a los registros de sucesos del sistema: proporciona acceso al registro de sucesos del sistema (SEL), al registro del DRAC 5 y a la pantalla de último bloqueo del sistema bloqueado, la cual no depende del estado del sistema operativo.
- 1 Integración de software de Dell OpenManage™: le permite iniciar la interfaz basada en web del DRAC5 desde Dell OpenManage Server Administrator o IT Assistant.
- 1 Alerta del RAC: le envía alertas sobre problemas potenciales con el nodo administrado por medio de mensajes de correo electrónico o con una captura SNMP mediante las configuraciones de NIC **Dedicado**, **Compartido con protección contra fallas** o **Compartido**.
- 1 Configuración local y remota: proporciona la configuración local y remota por medio de la utilidad de línea de comandos de RACADM.
- 1 Administración remota de la alimentación: ofrece funciones de administración remota de la alimentación desde una consola de administración, por ejemplo, de apagado y restablecimiento.
- 1 Compatibilidad con IPMI.
- 1 Cifrado de Capa de conexión segura (SSL): ofrece administración remota y segura del sistema por medio de la interfaz basada en web.
- 1 Administración de seguridad mediante niveles de contraseña: evita el acceso no autorizado a un sistema remoto.
- 1 Autoridad basada en funciones: proporciona permisos asignables para distintas tareas de administración de sistemas.

Otros documentos que puede necesitar

Además de esta *Guía del usuario*, los documentos siguientes proporcionan información adicional sobre la configuración y funcionamiento del DRAC 5 en su sistema:

- 1 La ayuda en línea del DRAC 5 proporciona información sobre el uso de la interfaz basada en web.
- 1 La *Guía del usuario de Dell OpenManage™ IT Assistant* y la *Guía de referencia de Dell OpenManage IT Assistant* proporcionan información sobre IT Assistant.
- 1 La *Guía del usuario de Dell OpenManage Server Administrator* proporciona información sobre la instalación y el uso de Server Administrator.
- 1 La *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage* ofrece información sobre cómo configurar el controlador de administración de la placa base (BMC), cómo configurar el sistema administrado con la Utilidad de administración de BMC e información adicional del BMC.
- 1 La *Guía del usuario de Dell Update Packages* ofrece información acerca de cómo obtener y utilizar los Dell Update Packages como parte de su estrategia de actualización del sistema.

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



La *Guía de información del producto* proporciona información importante de seguridad y normativas. La información de garantía se puede incluir en este documento o como documento independiente.

- 1 La *Guía de instalación de bastidor* y las *Instrucciones de instalación de bastidor* incluidas con su solución de bastidor describen cómo instalar su sistema en un bastidor.
- 1 La *Guía de introducción* proporciona una descripción general de las características del sistema, de cómo instalar el sistema y la especificaciones técnicas.
- 1 El *Manual del propietario del hardware* proporciona información sobre las características del sistema y describe cómo solucionar los problemas del sistema y cómo instalar o sustituir los componentes del mismo.
- 1 La documentación de Systems Management Software describe las características, requisitos, instalación y funcionamiento básico del software.
- 1 La documentación del sistema operativo describe cómo instalar (si es necesario), configurar y utilizar el software del sistema operativo.
- 1 La documentación de cualquier componente adquirido de forma independiente proporciona información para configurar e instalar estas opciones.
- 1 A veces se incluyen actualizaciones con el sistema para describir cambios en el sistema, el software o la documentación.



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

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

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Instalación del sistema operativo por medio de VM-CLI

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Antes de comenzar](#)
- [Creación de un archivo de imagen iniciable](#)
- [Preparación para la instalación](#)
- [Instalación del sistema operativo](#)

La utilidad de interfaz de línea de comandos de medios virtuales (VM-CLI) es una interfaz de línea de comandos que ofrece las 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 con secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad VM-CLI en la red de su empresa.

Antes de comenzar

Antes de usar la utilidad VM-CLI, asegúrese que los sistemas remotos de destino y la red de la empresa cumplan con los requisitos que se listan en las secciones siguientes.

Requisitos de los sistemas remotos

- 1 La tarjeta DRAC 5 debe estar instalada en cada sistema remoto
- 1 El dispositivo virtual en cada sistema remoto debe ser el primer dispositivo en el orden de inicio del BIOS.

Integración personalizada de fábrica de Dell

Cuando usted pide el sistema Dell utilizando las opciones de Integración personalizada de fábrica de Dell (CFI), Dell puede preconfigurar el sistema con una tarjeta DRAC 5 que incluya un nombre DDNS y un BIOS de sistema preconfigurado que esté habilitado para medios virtuales. Con esta configuración, el sistema estará listo para iniciar a partir de los dispositivos de medios virtuales al momento de instalarlo en la red de su empresa.

Para obtener más información, consulte el sitio web de Dell en www.dell.com.

Requisitos de red

Una área compartida de red debe tener los componentes siguientes:

- 1 Los archivos de sistema operativo
- 1 Los archivos controladores requeridos
- 1 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, asegúrese que un sistema admitido pueda iniciarse a partir del archivo. Para probar el archivo de imagen, transfíralo a un sistema de prueba por medio de la interfaz de usuario web del DRAC 5 y luego reinicie el sistema.

Las secciones a continuación proporcionan información específica para crear archivos de imagen para sistemas Windows y Linux.

Creación de un archivo de imagen para sistemas Linux

Use la utilidad de duplicador de datos para crear un archivo de imagen iniciable para el sistema Linux.

Para ejecutar la utilidad, abra una ventana de símbolo del sistema y escriba lo siguiente:

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

Por ejemplo:

```
dd if=/dev/fd0 of=myfloppy.img
```

Creación de un archivo de imagen para sistemas Windows

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

Preparación para la instalación

Configuración de los sistemas remotos

1. Cree una área compartida de red a la que la estación de administración pueda tener acceso.
2. Copie los archivos de sistema operativo en la área compartida de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

Si no tiene un archivo de imagen iniciable preconfigurado para instalación, prepárelo. Incluya los programas o secuencias de comandos que se vayan a utilizar para los procedimientos de instalación del sistema operativo

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

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

1. Siga procedimientos estándares de instalación basada en red
 1. Marque la imagen de instalación como "de sólo lectura" para asegurarse que cada sistema de destino se inicie y ejecute el mismo procedimiento de instalación
4. Realice uno de los procedimientos siguientes:
 1. Integre la utilidad RACADM y la interfaz de línea de comandos de medios virtuales (VM-CLI) en la aplicación existente de instalación del sistema operativo. Utilice el ejemplo de secuencia de comandos de distribución como guía cuando integre las utilidades del DRAC 5 en la aplicación existente de distribución de sistemas operativos.
 1. Use la secuencia de comandos **vmdeploy** existente para instalar el sistema operativo.
-

Instalación del sistema operativo

Use la 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 requisitos detallados para instalar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para instalar el sistema operativo en los sistemas remotos de destino.

1. Identifique los sistemas remotos que recibirán la instalación.
 2. Tome nota de los nombres de DRAC 5 y de las direcciones IP de los sistemas remotos de destino.
 3. Realice el procedimiento siguiente para cada sistema remoto de destino:
 - a. Configure un proceso de VM-CLI que incluya los siguientes parámetros para el sistema de destino:
 - o Dirección IP de DRAC 5 o nombre DDNS
 - o Nombre del archivo de imagen iniciable de instalación
 - o Nombre de usuario de DRAC 5
 - o Contraseña de usuario de DRAC 5
 - b. Por medio de RACADM, establezca la opción **iniciar una vez** para el DRAC 5 de destino.
 - c. Por medio de RACADM, reinicie el sistema del DRAC 5.
-

[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

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Compatibilidad con el SM-CLP de DRAC 5](#)
- [Funciones del SM-CLP](#)

Esta sección ofrece información acerca del Protocolo de línea de comandos de administración de servidor (SM-CLP) del Grupo de trabajo de administración de servidor (SMGW) que está incorporado en el DRAC 5.

NOTA: Esta sección supone que usted está familiarizado con la iniciativa de Arquitectura de administración de sistemas para hardware de servidores (SMASH) y con las especificaciones del SM-CLP de SMWG. Para obtener más información sobre estas especificaciones, consulte el sitio web del Grupo de trabajo de administración distribuida (DMTF) en www.dmtf.org.

El SM-CLP de DRAC 5 es un protocolo impulsado por el DMTF y el SMWG para proporcionar estándares para las implementaciones de interfaz de línea de comandos para administración de sistemas. Se están realizando muchos esfuerzos para lograr el objetivo de tener una arquitectura SMASH definida que constituya los cimientos para un conjunto de componentes de administración de sistemas más estandarizado. El SM-CLP de SMWG es un subcomponente de los esfuerzos generales de SMASH que el DMTF está impulsando.

Compatibilidad con el SM-CLP de DRAC 5

El DRAC 5 es el primer producto de RAC que ofrece compatibilidad con el protocolo de línea de comandos basado en el estándar SM-CLP. El SM-CLP se aloja en el firmware del controlador DRAC 5 y es compatible con las interfaces basadas en Telnet, SSH y serie. La interfaz de SM-CLP del DRAC 5 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por la organización DMTF.

Las secciones siguientes proporcionan una descripción de la característica de SM-CLP que se aloja en el DRAC 5.

Características de SM-CLP

La especificación SM-CLP proporciona un conjunto común de verbos estándares de SM-CLP que se pueden usar para la administración simple de sistemas por medio de la CLI.

La [tabla 11-1](#) proporciona una lista de los verbos admitidos de la CLI.

Tabla 11-1. Verbos admitidos de la CLI

| Verbo | Definición |
|---------|--|
| cd | Navega el mapa usando el shell. |
| delete | Elimina la instancia de un objeto. |
| help | Muestra la ayuda de un destino específico. |
| reset | Restablece el destino. |
| show | Muestra los subdestinos, las propiedades y los verbos del destino. |
| start | Enciende un destino. |
| stop | Apaga un destino. |
| exit | Cierra la sesión del shell de SM-CLP. |
| version | Muestra los atributos de versión de un destino. |

Destinos y operaciones de administración de SM-CLP

El SM-CLP promueve el concepto de verbos y destinos para ofrecer capacidades de administración de sistemas por medio de la CLI. El verbo indica la operación a realizar y el destino determina la entidad (u objeto) que ejecuta la operación.

A continuación se muestra un ejemplo de la sintaxis de línea de comandos del SM-CLP.

```
<verbo> [<opciones>] [<destino>] [<propiedades>]
```

Durante una sesión típica de SM-CLP, el usuario puede realizar operaciones con los verbos que se listan en la [tabla 11-1](#).

Operaciones de administración

El SM-CLP del DRAC 5 permite a los usuarios administrar lo siguiente:

- 1 Administración de la alimentación de servidor: encender, apagar o reiniciar el sistema
- 1 Administración del registro de sucesos del sistema (SEL): muestra o borra las anotaciones del SEL

Destinos

La [tabla 11-2](#) proporciona una lista de los destinos que se ofrecen a través del SM-CLP para ejecutar estas operaciones.

Tabla 11-2. Destinos de SM-CLP

| Destino | Definición |
|---|--|
| /sistema1 | El sistema administrado de destino. |
| /sistema1/registros1 | El destino de la recolecciones de registro |
| /sistema1/registros1/registro1 | El destino del registro de sucesos del sistema (SEL) del sistema administrado. |
| /sistema1/registros1/registro1/anotación1 | Una instancia individual de anotación del SEL en el sistema administrado. |

Opciones

La [tabla 11-3](#) muestra una lista de las opciones admitidas de SM-CLP.

Tabla 11-3. Opciones admitidas de SM-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. |

Formato de los mensajes de salida de SM-CLP

El DRAC 5 es compatible actualmente con los mensajes de salida de texto según se describe en las especificaciones del SM-CLP.

Ejemplos de SM-CLP de DRAC 5

Los apartados siguientes contienen escenarios de ejemplo para usar el SM-CLP para ejecutar las operaciones siguientes:

- 1 Administración de la alimentación del servidor
- 1 Administración del SEL
- 1 Navegación del mapa de destino
- 1 Mostrar las propiedades del sistema

Administración de la alimentación del servidor

La [tabla 11-4](#) muestra ejemplos de cómo usar el SM-CLP para realizar operaciones de administración de la alimentación en un sistema administrado.

Tabla 11-4. Operaciones de administración de la alimentación del servidor

| Operación | Sintaxis |
|--|---|
| Iniciar sesión en el RAC por medio de la interfaz Telnet/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) 2004-2006 Dell, Inc. All Rights Reserved -> |
| Apagar el servidor | - ->stop /system1 system1 has been stopped successfully |

| | |
|---|--|
| Encender el servidor a partir de un estado de apagado | - ->start /systeml systeml has been started successfully |
| Reiniciar el servidor | ->reset /systeml systeml has been reset successfully |

Administración del SEL

La [tabla 11-5](#) muestra ejemplos de cómo usar el SM-CLP para realizar operaciones relacionadas con el registro de sucesos del sistema en el sistema administrado.

Tabla 11-5. Operaciones de administración del SEL

| Operación | Sintaxis |
|--------------------------|--|
| Ver el SEL | <pre>->show /systeml/logsl/logl /systeml/logsl/logl 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</pre> |
| Ver la anotación del SEL | <pre>->show /systeml/logsl/logl/record4 /systeml/logsl/logl/record4: Properties: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 200506200100512.000000-000 Description = FAN 7 RPM: fan sensor, detected a failure ElementName = IPMI SEL Record Commands: cd show help exit version</pre> |
| Borrar el SEL | <pre>->delete /systeml/logsl/logl/record* All records deleted successfully</pre> |

Navegación del mapa de destino

La [tabla 11-6](#) muestra ejemplos de cómo usar el verbo `cd` para navegar el mapa. En todos los ejemplos, se asume que el destino predeterminado inicial es `/`.

Tabla 11-6. Operaciones de navegación del mapa de destino

| Operación | Sintaxis |
|---|---------------|
| Desplazarse al sistema de destino y reiniciarlo | ->cd sistema1 |

| | |
|---|---|
| | ->reset |
| | NOTA: El destino predeterminado actual es /. |
| Desplazarse al registro 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 11-7](#) muestra una lista de las propiedades del sistema que aparecen cuando el usuario escribe lo siguiente:

```
show /system1
```

Estas propiedades se obtienen del perfil de sistema base proporcionado por el cuerpo de estándares y se basa en la clase CIM_ComputerSystem según lo define el esquema CIM.

Para obtener información adicional, consulte las definiciones del esquema CIM de DMTF.

Tabla 11-7. Propiedades del sistema

| Objeto | Propiedad | Descripción |
|--------------------|-------------|--|
| CIM_ComputerSystem | Nombre | Identificador único de la instancia de un sistema que existe en el entorno empresarial. MaxLen = 256 |
| | ElementName | Nombre mnemotécnico para el 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, WVN, NAA |
| | Dedicado | Enumeración que indica si el sistema es un sistema de uso específico o un sistema de uso general. Valores: 0=No dedicado 1=Desconocido 2=Otro 3=Almacenamiento 4=Enrutador 5=Conmutador 6=Conmutador de capa 3 7=Conmutador de oficina central 8=Concentrador 9=Acceder al servidor 10=Servidor de seguridad 11=Imprimir 12=E/S 13=Almacenamiento en caché de web 14=Administración 15=Bloquear servidor 16=Servidor de archivos |

| | | |
|--|-------------------|---|
| | | <p>17=Dispositivo portátil de usuario,</p> <p>18=Repetidor</p> <p>19=Puente/extensión</p> <p>20=Puerta de enlace</p> <p>21=Virtualizador de almacenamiento</p> <p>22=Biblioteca de medios</p> <p>23=Nodo extensor</p> <p>24=Cabezal de NAS</p> <p>25=NAS autónomo</p> <p>26=Fuente de alimentación ininterrumpible</p> <p>27=Teléfono de IP</p> <p>28=Controlador de administración</p> <p>29=Administrador de chasis</p> |
| | ResetCapability | <p>Define los métodos de restablecimiento disponibles en el sistema</p> <p>Valores:</p> <p>1=Otro</p> <p>2=Desconocido</p> <p>3=Desactivado</p> <p>4=Activado</p> <p>5=No implementado</p> |
| | CreationClassName | La superclase de la cual se obtiene esta instancia. |
| | EnabledState | <p>Indica los estados activado o desactivado del sistema.</p> <p>Valores:</p> <p>0=Desconocido</p> <p>1=Otro</p> <p>2=Activado</p> <p>3=Desactivado</p> <p>4=Apagando</p> <p>5=No aplicable</p> <p>6=Activado pero fuera de línea</p> <p>7=En prueba</p> <p>8=Diferido</p> <p>9=En reposo</p> <p>10=Iniciando</p> |
| | EnabledDefault | <p>Indica la configuración predeterminada de arranque para el estado activado del sistema. De manera predeterminada, el sistema está "Activado" (valor=2).</p> <p>Valores:</p> <p>2=Activado</p> <p>3=Desactivado</p> <p>4=No aplicable</p> <p>5=Activado pero fuera de línea</p> <p>6=Sin valor predeterminado</p> |
| | RequestedState | <p>Indica el último estado solicitado o deseado para el sistema.</p> <p>Valores:</p> <p>2=Activado</p> |

| | | |
|--|-------------------|--|
| | | <p>3=Desactivado</p> <p>4=Apagar</p> <p>5=Sin cambio</p> <p>6=Fuera de línea</p> <p>7=Probar</p> <p>8=Diferido</p> <p>9=En reposo</p> <p>10=Reiniciar</p> <p>11=Restablecer</p> <p>12=No aplicable</p> |
| | HealthState | <p>Indica la condición actual del sistema.</p> <p>Valores:</p> <p>0=Desconocido</p> <p>5=En buen estado</p> <p>10=Degradado/advertencia</p> <p>15=Falla menor</p> <p>20=Falla mayor</p> <p>30=Falla crítica</p> <p>35=Error no recuperable</p> |
| | OperationalStatus | <p>Indica el estado actual del sistema.</p> <p>Valores:</p> <p>0=Desconocido</p> <p>1=Otro</p> <p>2=En buen estado</p> <p>3=Degradado</p> <p>4=Bajo presión</p> <p>5=Falla predictiva</p> <p>6=Error</p> <p>7=Error no recuperable</p> <p>8=Iniciando</p> <p>9=Deteniendo</p> <p>10=Detenido</p> <p>11=En servicio</p> <p>12=Sin contacto</p> <p>13=Perdió la comunicación</p> <p>14=Anulado</p> <p>15=Durmiente</p> <p>16=Asistiendo a entidad con error</p> <p>17=Completado</p> <p>18=Modo de encendido</p> |
| | Descripción | Una texto de descripción del sistema. |

[Regresar a la página de contenido](#)

Solución de problemas

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

● [Solución de problemas del DRAC 5](#)

Solución de problemas del DRAC 5

Consulte las tablas a continuación para recibir ayuda con la solución de problemas del DRAC 5 y el comando RACADM:

La [tabla 6-8](#), "[Uso del DRAC 5 con Active Directory: Preguntas frecuentes](#)"

La [tabla 7-7](#), "[Uso de la redirección de consola: Preguntas frecuentes](#)"

La [tabla 8-2](#), "[Uso de los medios virtuales: Preguntas frecuentes](#)"

La [tabla 9-4](#), "[Uso de los comandos serie y racadm: Preguntas frecuentes](#)"

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Instalación y configuración de DRAC 5

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Antes de comenzar](#)
- [Instalación del hardware del DRAC 5](#)
- [Configuración del sistema para usar un DRAC 5](#)
- [Descripción de configuración e instalación de software](#)
- [Instalación del software en el sistema administrado](#)
- [Instalación del software en la estación de administración](#)
- [Configuración de un explorador de web admitido](#)
- [Configuración de propiedades del DRAC 5](#)
- [Configuración de valores de red del DRAC 5](#)
- [Adición y configuración de usuarios del DRAC 5](#)
- [Actualización del firmware del DRAC 5](#)
- [Acceso al DRAC 5 a través de una red](#)
- [Configuración de IPMI](#)
- [Configuración de los sucesos de plataforma](#)

Esta sección proporciona información sobre cómo instalar y configurar el hardware y software del DRAC 5.

Antes de comenzar

Reúna los elementos siguientes que se incluyeron con el sistema antes de instalar y configurar el software del DRAC 5:

1. Hardware del DRAC 5 (ya instalado o en el paquete opcional)
1. Procedimientos de instalación del DRAC 5 (se encuentran en este capítulo)
1. CD Dell™ PowerEdge™ *Installation and Server Management*
1. CD Dell *Systems Management Consoles*
1. CD Dell *PowerEdge Service and Diagnostic Utilities*
1. CD Dell *PowerEdge Documentation*

Instalación del hardware del DRAC 5

 **NOTA:** La conexión del DRAC 5 emula una conexión de teclado USB. Por consiguiente, cuando reinicia el sistema, éste no le notificará si el teclado no está conectado.

El DRAC 5 se puede preinstalar en su sistema o está disponible de forma independiente en un paquete. Para comenzar con el DRAC 5 que ya está instalado en su sistema, consulte "[Descripción de la configuración e instalación del software](#)".

Si no hay un DRAC 5 instalado en su 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 su plataforma para obtener instrucciones de instalación del hardware.

 **NOTA:** Para obtener información sobre cómo quitar el DRAC 5, consulte la *Guía de instalación y solución de problemas* que se incluye con el sistema. Asimismo, revise todas las propiedades de RAC de Microsoft® Active Directory® asociadas con el DRAC 5 que se retiró, para asegurar que se tiene una seguridad apropiada.

Configuración del sistema para usar un DRAC 5

Para configurar el sistema para usar un DRAC 5, use la utilidad de configuración de acceso remoto de Dell (anteriormente conocida como el módulo de configuración de BMC).

Para ejecutar la utilidad de configuración de acceso remoto de Dell, realice los pasos a continuación:

1. Conecte o reinicie el sistema.
2. Presione <Ctrl><E> cuando se le pida durante la POST.

Si el sistema operativo comienza a cargarse antes de que usted presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el sistema e inténtelo otra vez.

3. Configure el NIC.
 - a. Con la tecla de flecha descendente, resalte **Selección de NIC**.
 - b. Con las teclas de flecha izquierda y derecha, seleccione una de las siguientes opciones del NIC:
 - **Dedicado:** seleccione esta opción para permitir que el dispositivo de acceso remoto utilice la interfaz de red dedicada que está disponible en el Remote Access Controller (RAC). Esta interfaz no se comparte con el sistema operativo host y envía el tráfico de administración a una red física separada, permitiéndole estar separada del tráfico de las aplicaciones. Esta opción sólo está disponible cuando hay una tarjeta DRAC instalada en el sistema.
 - **Compartido:** seleccione esta opción para compartir la interfaz de red con el sistema operativo host. La interfaz de red del dispositivo de acceso remoto funciona sin restricciones cuando el sistema operativo host está configurado para modo colaborativo de NIC. El dispositivo

de acceso remoto recibe datos por medio del NIC 1 y del NIC 2, pero transmite datos únicamente por medio del NIC 1. Si el NIC 1 falla, no se podrá acceder al dispositivo de acceso remoto.

- o **Protección contra fallos:** seleccione esta opción para compartir la interfaz de red con el sistema operativo host. La interfaz de red del dispositivo de acceso remoto funciona sin restricciones cuando el sistema operativo host está configurado para modo colaborativo de NIC. El dispositivo de acceso remoto recibe datos por medio del NIC 1 y del NIC 2, pero transmite datos únicamente por medio del NIC 1. Si el NIC 1 falla, el dispositivo de acceso cederá sus funciones al NIC 2 en lo que respecta a toda la transmisión de datos. El dispositivo de acceso remoto seguirá usando el NIC 2 para la transmisión de información. Si el NIC 2 falla, el dispositivo de acceso remoto devolverá todas las funciones de transmisión de datos al NIC 1.

4. Configure los parámetros de LAN del controlador de red para que utilicen DHCP o una fuente de direcciones IP estática.
 - a. Usando la tecla de flecha descendente, seleccione **Parámetros de LAN** y presione <Entrar>.
 - b. Usando las teclas de flecha ascendente y descendente, seleccione **Fuente de dirección IP**.
 - c. Usando las teclas de flecha a la derecha y a la izquierda, seleccione DHCP o **Estática**.
 - d. Si selecciona **Estática**, configure los valores para **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada**.
 - e. Oprima <Esc>.

5. Oprima <Esc>.

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

El sistema se reiniciará automáticamente.

Consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base de Dell OpenManage™* para ver más información sobre la utilidad de configuración de acceso remoto de Dell.

Descripción de configuración e instalación de software

Esta sección ofrece una descripción de alto nivel de la instalación del software del DRAC 5 y del proceso de configuración. 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 el software del DRAC 5

Para instalar el software del DRAC 5, realice los pasos siguientes en el orden indicado:

1. Instalar el software en el sistema administrado. Consulte "[Instalación del software en el sistema administrado](#)".
2. Instalar el software en la estación de administración. Consulte "[Instalación del software en la estación de administración](#)".

Configuración del DRAC 5

Para configurar el software del DRAC 5, realice los pasos siguientes en el orden indicado:

1. Seleccione una de las siguientes herramientas de configuración:
 - 1 Interfaz basada en web
 - 1 CLI de RACADM
 - 1 Consola de conexión serie/Telnet/SSH

 **NOTA:** Si usa más de una herramienta de configuración del DRAC 5 al mismo tiempo, puede obtener resultados inesperados.

2. Configure los valores de red del DRAC 5. Consulte "[Configuración de valores de red del DRAC 5](#)".
 3. Agregue y configure usuarios del DRAC 5. Consulte "[Adición y configuración de usuarios del DRAC 5](#)".
 4. Configure el explorador de web para poder 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 Reinicio automático de Windows](#)".
 6. Actualice el firmware del DRAC 5. Consulte "[Actualización del firmware del DRAC 5](#)".
 7. Acceda al DRAC 5 por medio de una red. Consulte "[Acceso al DRAC 5 a través de una red](#)".
-

Instalación del software en el sistema administrado

La instalación del software en el sistema administrado es opcional. Sin el software Managed System, se pierde la capacidad de utilizar el comando RACADM localmente y el RAC no podrá capturar la pantalla de último bloqueo.

Para instalar el software Managed System, instale el software en el sistema administrado con el CD *Dell PowerEdge Installation and Server Management*. Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida*.

El software Managed System instala en el sistema administrado las opciones que usted seleccionó de la versión correspondiente de Server Administrator.

 **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, no podrá ver la pantalla de último bloqueo del sistema ni usar la función de **Recuperación automática**.

Para obtener más información sobre la pantalla de último bloqueo, consulte "[Visualización de la pantalla de último bloqueo del sistema](#)".

Configuración del sistema administrado para capturar la pantalla de último bloqueo

Antes de que el DRAC 5 pueda capturar la pantalla de último bloqueo, debe configurar el sistema administrado con los requisitos previos siguientes.

1. Instale el software Managed System. Para obtener más información acerca de cómo instalar el software Managed System, consulte la *Guía del usuario de Server Administrator*.
2. Ejecute un sistema operativo Microsoft® Windows® admitido con la función de "reiniciar automáticamente" de Windows desactivada en la **Configuración de inicio y de recuperación de Windows**.
3. Active la pantalla de último bloqueo (está desactivada de manera predeterminada).

Para activarla por medio de RACADM local, abra una ventana de símbolo de sistema y escriba los comandos siguientes:

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

4. Active el temporizador de recuperación automática y establezca la acción de **Recuperación automática** en **Restablecer**, **Apagar** o **Ciclo de encendido**. Para configurar el temporizador de **Recuperación automática**, debe utilizar Server Administrator o IT Assistant.

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

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

Desactivación de la opción Reinicio automático de Windows

Para asegurarse de que la función de pantalla de último bloqueo de la interfaz basada en web del DRAC 5 funciona correctamente, debe desactivar la opción **Reinicio automático** en los sistemas administrados que ejecutan los sistemas operativos Microsoft Windows Server 2003 y Windows 2000 Server.

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

Desactivación de la opción 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 **Avanzado**.

3. Haga clic en el botón **Inicio y recuperación...**
4. Deseleccione la casilla de marcación **Reiniciar automáticamente**.

Instalación del software en la estación de administración

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

- 1 El CD *Dell PowerEdge Installation and Server Management*: un CD iniciable que proporciona las herramientas necesarias para configurar el sistema e instalar el sistema operativo. Este CD contiene los últimos productos de software para administración de sistemas, incluso los diagnósticos de Dell OpenManage Server Administrator, Storage Management y los servicios de acceso remoto.
- 1 El CD *Dell Systems Management Consoles*: contiene todos los últimos productos de consola de administración de sistemas de Dell, incluso el Dell OpenManage IT Assistant.
- 1 El CD *Dell PowerEdge Service and Diagnostic Utilities*: proporciona las herramientas necesarias para configurar el sistema e incluye el BIOS, firmware, diagnósticos y archivos controladores más recientes optimizados por Dell para su sistema.
- 1 El CD *Dell PowerEdge Documentation*: le ayuda a mantenerse actualizado con la documentación de sistemas, productos de software para administración de sistemas, periféricos y controladores RAID.

Para obtener información sobre la instalación del software de Server Administrator, consulte la *Guía del usuario de Server Administrator*.

Configuración de la estación de administración de Red Hat Enterprise Linux (versión 4)

El visor de KVM digital de Dell requiere una configuración adicional para poder funcionar en una estación de administración de Red Hat Enterprise Linux (versión 4). Al momento de instalar el sistema operativo Red Hat Enterprise Linux (versión 4) en la estación de administración, realice los procedimientos siguientes:

- 1 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 el visor de KVM digital de Dell en la estación de administración.
- 1 Para comprobar que el visor de KVM digital de Dell funciona correctamente, abra los puertos siguientes en el servidor de seguridad:
 - o El puerto de teclado y mouse (el puerto predeterminado es el 5900)
 - o El puerto de vídeo (el puerto predeterminado es el 5901)

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

Para usar las funciones de RACADM remoto, instale RACADM en una estación de administración con Linux.

 **NOTA:** Cuando se ejecuta **Setup** en el CD *Systems Management Consoles*, 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 donde desea instalar los componentes de Management Station.
2. Si es necesario, monte el CD *Dell Systems Management Consoles* por medio del comando siguiente o con un comando similar:

```
mount /media/cdrom
```

3. Desplácese al directorio `/linux/rac` y ejecute el comando siguiente:

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

Para recibir ayuda con el comando de RACADM, escriba `racadm help` después de ejecutar los comandos anteriores. Para obtener más información acerca de RACADM, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Desinstalación de RACADM

Para desinstalar RACADM, abra una ventana de símbolo del sistema y escriba:

```
rpm -e <nombre_del_paquete_racadm>
```

donde `<nombre_del_paquete_racadm>` es el paquete RPM que se utilizó para instalar el software del RAC.

Por ejemplo, si el nombre de paquete RPM es `srvadmin-racadm5`, escriba:

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

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 "[Exploradores de web admitidos](#)".

Configuración del explorador de web para conectarse a la interfaz basada en web

Si se conecta a la interfaz basada en web del DRAC 5 desde una estación de administración conectada a la Internet mediante un servidor proxy, debe configurar el explorador de web para que acceda a la Internet desde este servidor.

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

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

Visualización de versiones localizadas de la interfaz basada en web

La interfaz basada en web del DRAC 5 es compatible con los siguientes idiomas de sistemas operativos de Windows:

- 1 Francés
- 1 Alemán
- 1 Español
- 1 Japonés
- 1 Chino simplificado

Para ver una versión traducida de la interfaz basada en web del DRAC 5 en Internet Explorer, realice los pasos a continuación:

1. Haga clic en el menú **Herramientas** y seleccione **Opciones de Internet**.
2. En la ventana **Opciones de Internet**, haga clic en **Idiomas**.
3. En la ventana **Preferencias de idioma**, haga clic en **Agregar**.
4. En la ventana **Agregar idioma**, seleccione un idioma compatible.
Para seleccionar más de un idioma, presione <Ctrl>.
5. Seleccione su idioma preferido y haga clic en **Subir** para subir el idioma al inicio de la lista.
6. Haga clic en **Aceptar**.
7. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.

Configuración de propiedades del DRAC 5

Configure las propiedades del DRAC 5 (red, usuarios, alertas, etc.) por medio de la interfaz basada en web o de RACADM.

Para obtener más información sobre cómo utilizar la interfaz basada en web, consulte "[Acceso a la interfaz basada en web](#)". Para obtener más información sobre cómo usar RACADM en una conexión serie o Telnet, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

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:

- 1 Interfaz basada en web: consulte "[Configuración del NIC del DRAC 5](#)"
- 1 CLI de RACADM: consulte "[cfgLanNetworking](#)"
- 1 Utilidad de configuración de acceso remoto de Dell: consulte "[Configuración del sistema para usar un DRAC 5](#)"

 **NOTA:** Si va a instalar el DRAC 5 en un entorno de Linux, consulte "[Instalación de RACADM](#)".

Adición y configuración de usuarios del DRAC 5

Utilice una de las herramientas a continuación para agregar y configurar usuarios del DRAC 5:

- 1 Interfaz basada en web: consulte "[Adición y configuración de usuarios del DRAC 5](#)".
 - 1 CLI de RACADM: consulte "[cfgUserAdmin](#)".
-

Actualización del firmware del DRAC 5

Utilice uno de los métodos siguientes para actualizar el firmware del DRAC 5.

- 1 Interfaz basada en web: consulte "[Actualización del firmware del DRAC 5 por medio de la interfaz basada en web](#)".
- 1 CLI de RACADM: consulte "[fwupdate](#)".
- 1 Dell Update Packages: consulte la *Guía del usuario de Dell Update Packages* para ver información acerca de cómo obtener y utilizar Dell Update Packages como parte de su estrategia de actualización del sistema

Antes de comenzar

Antes de actualizar el firmware del DRAC 5 por medio de RACADM local o los Dell Update Packages, realice los procedimientos a continuación. De lo contrario, es posible que la operación de actualización del firmware sufra una falla.

1. Instale y active los controladores adecuados de IPMI y de nodo administrado.
2. Si el sistema ejecuta el sistema operativo Windows, active e inicie los servicios de Instrumental de administración de Windows (WMI).
3. Compruebe que la unidad flash virtual del RAC no esté siendo usada por el sistema operativo ni por otra aplicación.
4. Compruebe que la función USB esté activada.

Descarga del firmware del DRAC 5

Para actualizar el firmware del DRAC 5, descargue el firmware más reciente del sitio web de asistencia Dell Support en la dirección support.dell.com y guarde el archivo en el sistema local.

Con el paquete de firmware del DRAC 5, se incluyen los siguientes componentes de software:

- 1 Datos y código de firmware del DRAC 5 compilado
- 1 Imagen ROM de expansión
- 1 Interfaz basada en web, JPEG y otros archivos de datos de la interfaz de usuario
- 1 Archivos de configuración predeterminados

Utilice la página **Actualización del firmware** para actualizar el firmware del DRAC 5 a la revisión más reciente. Cuando ejecuta la actualización del firmware, ésta conserva la configuración actual del DRAC 5.

Actualización del firmware del DRAC 5 por medio de la interfaz basada en web

1. Abra la interfaz basada en web e inicie sesión en el sistema remoto.
Consulte "[Acceso la interfaz basada en web](#)".
2. En el árbol de **Sistema**, haga clic en **Acceso Remoto** y haga clic en la ficha **Actualizar**.

- En la página **Actualización del 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** desplazarse hasta la imagen.

 **NOTA:** Si está ejecutando 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**.

- Haga clic en **Actualizar**.

La actualización puede tardar varios minutos en completarse. Al concluir, aparecerá un cuadro de diálogo.

- Haga clic en **Aceptar** para cerrar la sesión y desconectarse automáticamente.
- Una vez restablecido el DRAC 5, haga clic en **Conectar** para iniciar sesión en el DRAC 5.

Cómo borrar la memoria caché del explorador

Después de la actualización del firmware, borre la memoria caché del explorador de web.

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

Acceso al DRAC 5 a través de una red

Una vez configurado el DRAC 5, puede acceder de forma remota al sistema administrado con una de las siguientes interfaces:

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

La [tabla 2-1](#) describe cada una de las interfaces del DRAC 5.

Tabla 2-1. Interfaces del DRAC 5

| Interfaz | Descripción |
|------------------------|---|
| Interfaz basada en web | Proporciona acceso remoto al DRAC 5 por medio de una interfaz gráfica de usuario. La interfaz basada en web está incorporada en el firmware del DRAC 5 y se puede acceder a ella por medio de la interfaz de NIC con un explorador de web admitido en la estación de administración. Para obtener una lista de exploradores de web admitidos, consulte " Exploradores de web admitidos ". |
| RACADM | Proporciona acceso remoto al DRAC 5 por medio de una interfaz de línea de comandos. RACADM utiliza la dirección IP del sistema administrado para ejecutar los comandos de RACADM (la opción de capacidad remota de RACADM [-r]). NOTA: La capacidad remota de RACADM sólo se admite en las estaciones de administración que ejecutan los sistemas operativos Windows 2000 Server, Windows XP Professional, Windows 2000 Professional, Windows Server 2003, Windows Server 2003 R2, Red Hat Enterprise Linux (versión 3 y versión 4) y Linux SUSE. |
| Consola Telnet | Proporciona acceso por medio del DRAC 5 al puerto del RAC de servidor e interfaces de administración de hardware a través del NIC del DRAC 5 y proporciona la compatibilidad para el uso de los comandos serie y RACADM, incluso los comandos powerdown , powerup , powercycle y hardreset . NOTA: Telnet es un protocolo no seguro que transmite todos los datos —incluso las contraseñas— como texto sin formato. Cuando transmita información confidencial, utilice la interfaz de SSH. |
| Interfaz de SSH | Proporciona las mismas capacidades que la consola Telnet mediante una capa de transporte cifrado para tener una mayor seguridad. |
| Interfaz de IPMI | Proporciona acceso por medio del DRAC 5 a los componentes básicos de administración del sistema remoto. La interfaz incluye IPMI en la LAN, IPMI en conexión serie y comunicación en serie en la LAN. Para obtener más información, consulte la <i>Guía del usuario del controlador de administración de la placa base de Dell OpenManage</i> . |

 **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 el NIC del DRAC 5 con un explorador de web admitido, o bien, mediante Server Administrator o IT Assistant.

Consulte "[Exploradores de web admitidos](#)" para ver una lista de los exploradores de web admitidos.

Para acceder al DRAC 5 a través de un explorador de web admitido, consulte "[Acceso a la interfaz basada en web](#)".

Para acceder a la interfaz de acceso remoto del DRAC 5 con Server Administrator, ejecute Server Administrator. En el árbol del sistema, en el panel izquierdo de la página de inicio de Server Administrator, haga clic en **Sistema** → **Chasis del sistema principal** → **Remote Access Controller**. Para obtener más información, consulte la Guía del usuario de Server Administrator.

Para obtener información sobre cómo acceder al DRAC 5 por medio de RACADM, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Configuración de IPMI

Esta sección ofrece información sobre cómo configurar y utilizar la interfaz IPMI del DRAC 5. La interfaz incluye lo siguiente:

- 1 IPMI en la LAN
- 1 IPMI en conexión serie
- 1 Comunicación en serie en la LAN

El DRAC5 es totalmente compatible con IPMI 2.0. Puede configurar la IPMI del DRAC por medio del explorador; por medio de una utilidad de código fuente abierto, como *ipmitool*; por medio del shell IPMI de Dell OpenManage, **ipmish**; o bien, por medio de RACADM.

Para obtener más información acerca de cómo utilizar el shell IPMI, *ipmish*, consulte la *Guía del usuario del BMC de Dell OpenManage™* que se encuentra en el sitio web de asistencia Dell Support en support.dell.com.

Para obtener más información acerca de cómo utilizar RACADM, consulte "[Uso de RACADM](#)".

Configuración de IPMI por medio de la interfaz 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. Configure la IPMI en la LAN.
 - a. En el árbol de **Sistema**, haga clic en **Acceso remoto**.
 - b. Haga clic en la ficha **Configuración** y haga clic en **Red**.
 - c. En la página **Configuración de la red** en **Configuración de la LAN de IPMI**, seleccione **Activar IPMI en la LAN** y haga clic en **Aplicar cambios**.
 - d. Actualice los privilegios de canal de LAN de IPMI, si es necesario.

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

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

- e. Defina la clave de cifrado de LAN de IPMI, si es necesario.

 **NOTA:** La IPMI del DRAC 5 es compatible con el protocolo RMCP+.

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

 **NOTA:** La clave de cifrado debe constar de 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 de **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 comunicación en serie en la LAN de IPMI.

 **NOTA:** Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de SOL sea idéntica a la velocidad en baudios del 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 necesita para usar la función de **Comunicación en serie en la LAN**.

Haga clic en el menú desplegable **Límite de nivel de privilegio del 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 de conexión serie**, cambie el modo de conexión serie de IPMI al valor adecuado.
En **Conexión serie de IPMI**, haga clic en el menú desplegable **Configuración del modo de conexión** y seleccione el modo adecuado.
 - c. Establezca la velocidad en baudios de la conexión serie de IPMI.
Haga clic en el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios adecuada y haga clic en **Aplicar cambios**.
 - d. Establezca el límite de nivel de privilegio del canal.
Haga clic en el menú desplegable **Límite de nivel de privilegio del canal**, seleccione **Administrador**, **Operador** o **Usuario**.
 - e. Haga clic en **Aplicar cambios**.
 - f. Asegúrese que el MUX serie este definido correctamente en el programa de configuración del BIOS del sistema administrado.
 - o Reinicie su sistema.
 - o Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
 - o Desplácese a **Comunicación serie**.
 - o En el menú **Conexión serie**, compruebe que **Conector serie externo** esté establecido como **Dispositivo de acceso remoto**.
 - o Guarde los cambios y salga del programa de configuración del BIOS.
 - o Reinicie su sistema.

Si la conexión serie de IPMI está en modo de terminal, usted puede configurar los siguientes valores adicionales:

- 1 Control de eliminación
- 1 Control del eco
- 1 Edición de línea
- 1 Nueva secuencia de línea
- 1 Introducir una nueva secuencia de línea

Para obtener más información sobre estas propiedades, consulte la especificación de 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](#)".
2. Configure la IPMI en la LAN.

Abra una petición de comandos, escriba el siguiente comando 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 de IPMI en la LAN. Para obtener más información, consulte las especificaciones de IPMI 2.0.

- a. Actualice los privilegios de canal de IPMI.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <nivel>
```

donde <nivel> es uno de los siguientes valores:

- o 2 (Usuario)
- o 3 (Operador)
- o 4 (Administrador)

Por ejemplo, para establecer el privilegio de canal de LAN de IPMI como 2 (Usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

- b. Defina la clave de cifrado de LAN de IPMI, si es necesario.

 **NOTA:** La IPMI del DRAC 5 es compatible con el protocolo RMCP+. Para obtener más información, consulte las especificaciones de IPMI 2.0.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>
```

donde <clave> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

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

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. Actualice el nivel de privilegio de mínimo de SOL IPMI.

El nivel de privilegio mínimo de SOL de IPMI determina el privilegio mínimo que se necesita para activar la comunicación en serie en la LAN de IPMI. Para obtener más información, consulte la especificación de IPMI 2.0.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>
```

donde <nivel> es uno de los siguientes valores:

- o 2 (Usuario)
- o 3 (Operador)
- o 4 (Administrador)

Por ejemplo, para definir los privilegios de IPMI como 2 (Usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. Actualice la velocidad en baudios de la comunicación en serie en la LAN de IPMI.

 **NOTA:** Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de SOL sea idéntica a la velocidad en baudios del sistema administrado.

En la petición de comandos, escriba el siguiente comando 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 comunicación en serie en la LAN.

 **NOTA:** La comunicación en serie en la LAN puede activarse o desactivarse individualmente para cada usuario.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

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

donde <identificación> es la identificación exclusiva del usuario.

4. Configure la conexión serie de IPMI.

a. Cambie el modo de conexión serie de IPMI por el valor adecuado.

En la petición de comandos, escriba el siguiente comando 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 siguiente comando 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 de hardware de la conexión serie de IPMI.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

- d. Establezca el nivel de privilegio mínimo de canal de conexión serie de IPMI.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <nivel>
```

donde <nivel> es uno de los siguientes valores:

- o 2 (Usuario)
- o 3 (Operador)
- o 4 (Administrador)

Por ejemplo, para establecer los privilegios de canal de conexión serie de IPMI como 2 (Usuario), escriba el comando siguiente:

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

- e. Asegúrese que el MUX serie este definido correctamente en el programa de configuración del BIOS.

- o Reinicie su sistema.
- o Durante la POST, presione <F2> para ingresar al programa de configuración del BIOS.
- o Desplácese a **Comunicación serie**.
- o En el menú **Conexión serie**, compruebe que **Conector serie externo** esté establecido como **Dispositivo de acceso remoto**.
- o Guarde los cambios y salga del programa de configuración del BIOS.
- o Reinicie su sistema.

Ha concluido la configuración de IPMI.

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**:

- o Control de eliminación
- o Control del eco
- o Edición de línea
- o Nueva secuencia de línea
- o Introducir una nueva secuencia de línea

Para obtener más información sobre estas propiedades, consulte la especificación de IPMI 2.0.

Configuración de sucesos de plataforma

La configuración de sucesos de plataforma ofrece un mecanismo para configurar el dispositivo de acceso remoto a fin de realizar acciones selectas ante ciertos mensajes de sucesos. Estas acciones incluyen reiniciar, realizar un ciclo de encendido, apagar y desencadenar una alerta (Captura de sucesos de plataforma [PET] y/o mensaje de correo electrónico).

Los sucesos de plataforma que se pueden filtrar incluyen los siguientes:

- 1 Falla de sonda del ventilador
- 1 Advertencia de sonda de baterías
- 1 Falla de sonda de baterías
- 1 Falla discreta de sonda de voltaje
- 1 Advertencia de sonda de temperatura
- 1 Falla de sonda de temperatura
- 1 Intromisión al chasis detectada
- 1 Redundancia degradada
- 1 Redundancia perdida
- 1 Advertencia del procesador
- 1 Falla del procesador
- 1 Procesador ausente
- 1 Advertencia PS/VRM/D2D
- 1 Falla PS/VRM/D2D
- 1 Suministro de energía ausente
- 1 Falla de registro de hardware
- 1 Recuperación de sistema automática

Cuando se presenta un suceso de plataforma (por ejemplo, la falla de una sonda de ventilador), se genera un suceso de sistema y se registra en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) de la lista de filtros de sucesos de plataforma en la interfaz basada en web y usted definió este filtro para generar una alerta (PET o mensaje de correo electrónico), se enviará una entonces una alerta de captura de suceso de plataforma o de mensaje de correo electrónico a un grupo establecido de uno o más destinos.

Si el mismo filtro de sucesos de plataforma también fue configurado para realizar una acción (por ejemplo, un reinicio del sistema), ésta se ejecutará.

Configuración de filtros del suceso de plataforma (PEF)

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

Configuración de PEF por medio de la interfaz de web de usuario

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 luego 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 alertas de filtro de sucesos de plataforma**.
4. En **Configuración de filtros de sucesos de plataforma**, seleccione la casilla **Activar alertas de filtro sucesos de plataforma** luego haga clic en **Aplicar cambios**.
5. En **Lista de filtros de sucesos de plataforma**, haga doble clic en el filtro que desea configurar.
6. En la página **Establecer sucesos de plataforma**, marque las selecciones que correspondan y luego haga clic en **Aplicar cambios**.

 **NOTA:** La opción **Generar alerta** debe estar activada para que la alerta se pueda enviar a los destinos válidos configurados. (PET o mensaje de correo electrónico).

Configuración de PEF por medio de la CLI de RACADM

1. Active el filtro de sucesos de plataforma.

Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
```

donde 1 y 1 son el índice del filtro de sucesos de plataforma y la selección de activar o desactivar, respectivamente.

El índice del PEF puede ser un valor de 1 a 17. La selección de activar o desactivar puede definirse como 1 (activado) ó 0 (desactivado).

Por ejemplo, para activar el filtro de sucesos de plataforma con el índice 5, escriba el comando siguiente:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. Configure las acciones del PEF.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <acción>
```

donde los bits de valores para <acción> son los siguientes:

- 1 Bit del valor 0 de <acción>: 1 = activar la acción de alerta, 0 = desactivar la alerta
- 1 Bit del valor 1 de <acción>: 1 = apagar; 0 = no apagar
- 1 Bit del valor 2 de <acción>: 1 = reiniciar; 0 = no reiniciar
- 1 Bit del valor 3 de <acción>: 1 = ejecutar ciclo de encendido; 0 = no ejecutar ciclo de encendido

Por ejemplo, para hacer que el filtro de sucesos de plataforma reinicie el sistema, escriba el comando siguiente:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
```

donde 1 es el índice del PEF y 2 es la acción de reiniciar del PEF.

Configuración de la PET

Configuración de la PET por medio de la interfaz de web de usuario

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte "[Acceso a la interfaz basada en web](#)".
2. Asegúrese que se siguieron los procedimientos descritos en "[Configuración del PEF por medio de la interfaz de web de usuario](#)".
3. Configure la política de la captura de sucesos de plataforma.
 - a. En la ficha **Administración de alertas**, haga clic en **Configuración de capturas**.
 - b. En **Valores de configuración del destino**, introduzca la información adecuada en el campo **Cadena de comunidad** y luego haga clic en **Aplicar cambios**.
4. Configure la dirección IP de destino de la captura de sucesos de plataforma
 - 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 de destino válida para la captura de sucesos de plataforma.
 - d. Haga clic en **Aplicar cambios**.
 - e. Haga clic en **Enviar captura de prueba** para probar la alerta configurada (si lo desea).

 **NOTA:** Para que pueda realizar este procedimiento, la cuenta de usuario debe tener permiso para **Probar alertas**. Consulte la [tabla 4-8](#).

- f. Repita los pasos "a" a "e" para los números de destino restantes.

Configuración de la PET por medio de la CLI de RACADM

1. Active las alertas globales.

Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Active la captura de sucesos de plataforma.

En la petición de comandos, escriba los siguientes comandos y presione <Entrar> después de cada uno de ellos:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
```

donde 1 y 1 son el índice del destino de la captura de sucesos de plataforma y la selección de activar o desactivar, respectivamente.

El índice del destino de la captura de sucesos de plataforma puede ser un valor de 1 a 4. La selección de activar o desactivar puede definirse como 1 (activado) ó 0 (desactivado).

Por ejemplo, para activar la captura de sucesos de plataforma con el índice 4, escriba el comando siguiente:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
```

3. Configure la política de la captura de sucesos de plataforma.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <dirección_IP>
```

donde 1 es el índice del destino de la captura de sucesos de plataforma y <dirección_IP> es la dirección IP del destino del sistema que recibe las alertas de sucesos de plataforma.

4. Configure la cadena de nombre de comunidad.

En la petición de comandos, escriba:

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <Nombre>
```

Configuración de las alertas de correo electrónico

Configuración de las alertas de correo electrónico por medio de la interfaz de web de usuario

1. Inicie sesión en el sistema remoto por medio de un explorador de web admitido. Consulte "[Acceso a la interfaz basada en web](#)".
 2. Asegúrese que se siguieron los procedimientos descritos en "[Configuración del PEF por medio de la interfaz de web de usuario](#)".
 3. Defina la configuración de la alerta de correo electrónico.
 - a. En la ficha **Administración de alertas**, haga clic en **Configuración de la alerta de correo electrónico**.
 - b. En **Configuración de la dirección del servidor SMTP (correo electrónico)**, introduzca la información adecuada en el campo **Dirección del servidor SMTP (correo electrónico)** y después haga clic en **Aplicar cambios**.
 4. Configure el destino de la alerta de correo electrónico.
 - a. En la columna **Número de alerta por correo electrónico**, haga clic en un número de alerta de 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 necesario).
 - e. Haga clic en **Aplicar cambios**.
 - f. Haga clic en **Enviar correo electrónico de prueba** para probar la alerta de correo electrónico configurada (si lo desea).
-  **NOTA:** Para que pueda realizar este procedimiento, la cuenta de usuario debe tener permiso para **Probar alertas**. Consulte la [tabla 4-8](#).
- g. Repita los pasos [a](#) a [e](#) para las configuraciones restantes de alertas de correo electrónico.
5. Active las alertas globales.
 - a. Haga clic en **Administración de alertas** y seleccione **Sucesos de plataforma**.
 - b. Seleccione la casilla **Activar alertas de filtro de sucesos de plataforma**.

Configuración de las alertas de correo electrónico por medio de la CLI de RACADM

1. Active las alertas globales.

Abra una petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```

2. Active las alertas por correo electrónico.

En la petición de comandos, escriba los siguientes comandos y presione <Entrar> después de cada uno de ellos:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
```

donde 1 y 1 son el índice del destino del mensaje de correo electrónico y la selección de activar o desactivar, respectivamente.

El índice del destino del mensaje de correo electrónico puede ser un valor de 1 a 4. La selección de activar o desactivar puede definirse como 1 (activado) ó 0 (desactivado).

Por ejemplo, para activar el correo electrónico con el índice 4, escriba el comando siguiente:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 0
```

3. Defina la configuración de correo electrónico.

En la petición de comandos, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>
```

donde 1 es el índice del destino del mensaje de correo electrónico y <dirección_de_correo_electrónico> es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

Para definir un mensaje personalizado, en el símbolo del sistema, escriba el siguiente comando y presione <Entrar>:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <mensaje_personalizado>
```

donde 1 es el índice del destino del mensaje de correo electrónico y <mensaje_personalizado> es el mensaje personalizado.

[Regresar a la página de contenido](#)

Configuración y uso de la consola de línea de comandos del DRAC 5

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Características de la consola de línea de comandos](#)
- [Activación y configuración del sistema administrado para utilizar una consola Telnet o serie](#)
- [Uso de Secure Shell \(SSH\)](#)
- [Habilitación de las opciones de seguridad adicionales del DRAC 5](#)
- [Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet \(sistema cliente\)](#)
- [Conexión del cable DB-9 para la consola serie](#)
- [Configuración del software de emulación de terminal de la estación de administración](#)
- [Uso de una consola Telnet o serie](#)

Esta sección proporciona información acerca de las características de la consola de línea de comandos (o la *consola de conexión serie/Telnet/SSH*) del DRAC 5 y explica cómo configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola.

Características de la consola de línea de comandos

EL DRAC 5 admite las siguientes características de consola Telnet y serie:

- 1 Una conexión de cliente serie y hasta cuatro conexiones simultáneas de cliente Telnet
- 1 Hasta cuatro conexiones simultáneas de cliente SSH
- 1 Acceso a las consolas del sistema administrado mediante el puerto serie del sistema y el NIC del DRAC 5
- 1 Comandos de consola que permiten encender, apagar, realizar un ciclo de encendido, restablecer, ver registros o configurar el DRAC 5
- 1 Admite el comando **RACADM**, que es útil para el uso de secuencias de comandos
- 1 Historial y edición de línea de comandos
- 1 El comando serie **connect com2** para conectar, ver e interactuar con la consola de texto del sistema administrado cuya salida se transmite por un puerto serie (incluso el BIOS y el sistema operativo)

 **NOTA:** Si está ejecutando Linux en el sistema administrado, el comando serie **connect com2** proporciona una verdadera interfaz de consola de Linux.

- 1 Control del tiempo de espera de las sesiones en todas las interfaces de consola

Activación y configuración del sistema administrado para utilizar una consola Telnet o serie

Los apartados siguientes proporcionan información sobre cómo activar y configurar una consola serie, Telnet o SSH en el sistema administrado.

Uso del comando serie connect com2

Cuando se usa el comando serie **connect com2**, se deben configurar correctamente los siguientes valores:

- 1 El valor de **Comunicación serie** → **Puerto serie** en el programa **Configuración del BIOS**.
- 1 Los valores de configuración del DRAC.

Cuando se establece una sesión Telnet con el DRAC 5 y esta configuración es incorrecta, es posible que el comando **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 de **Configuración del BIOS** para redirigir la salida a un puerto serie.

 **NOTA:** Debe configurar el programa **Configuración del sistema** en combinación con el comando **connect com2**.

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

<F2> = System Setup

3. Desplácese y seleccione **Comunicación serie** presionando <Entrar>.
4. Establezca los siguientes valores para la pantalla **Comunicación serie**:
Conector serie externo: Dispositivo de acceso remoto
Redirección después de inicio: Desactivado
5. Presione <Esc> para salir del programa de **configuración del sistema** y completar la configuración del mismo.

Uso de la interfaz serie de acceso remoto

Al establecer una conexión serie con el dispositivo de RAC, se dispone de las siguientes interfaces:

- 1 Interfaz serie de IPMI
- 1 Interfaz serie del RAC

Interfaz serie de IPMI

En la interfaz serie de IPMI, están disponibles los siguientes modos:

- 1 **Modo de terminal de IPMI**: admite comandos ASCII que se envíen desde una terminal de conexión serie. El conjunto de comandos se limita a un número restringido de comandos (incluso el control de alimentación) y admite comandos simples de IPMI que se introduzcan como caracteres hexadecimales ASCII.
- 1 **Modo básico de IPMI**: admite una interfaz binaria para acceso del 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, realice los pasos a continuación:

1. Desactive la interfaz serie del RAC.

En la petición de comandos, escriba:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

2. Active el modo adecuado de IPMI.

Por ejemplo, en el símbolo del sistema, 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 más información.

Interfaz serie del RAC

El RAC también admite una interfaz de consola serie (o *consola serie del RAC*) que proporciona una CLI de RAC que no está definida por IPMI. Si el sistema incluye una tarjeta RAC con la **Consola serie** activada, la tarjeta de RAC suprimirá la configuración de la conexión serie de IPMI y mostrará la interfaz serie de la CLI del RAC.

Para activar la interfaz de terminal serie del RAC, establezca la propiedad **cfgSerialConsoleEnable** como **1** (VERDADERO).

Por ejemplo:

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

Para obtener más información, consulte "[cfgSerialConsoleEnable \(lectura/escritura\)](#)".

La [tabla 3-1](#) muestra la configuración de la interfaz serie.

Tabla 3-1. Configuración de la interfaz serie

| Modo de IPMI | Consola serie del RAC | Interfaz |
|--------------|-----------------------|-----------------------|
| Básico | Desactivado | Modo básico |
| Básico | Activado | CLI del RAC |
| Terminal | Desactivado | Modo de terminal IPMI |
| Terminal | Activado | CLI del RAC |

Configuración de Linux para la redirección de consola durante el inicio

Los pasos siguientes son específicos para el GRand Unified Bootloader (GRUB) de Linux. Cambios similares serían necesarios si se usa un cargador de inicio diferente.

 **NOTA:** Al configurar la ventana de emulación VT100 cliente, usted debe configurar la ventana o la aplicación que muestra la consola redirigida con 25 filas x 80 columnas para asegurar que se muestre el texto correctamente; de lo contrario, algunas pantallas de texto pueden aparecer ilegibles.

Modifique el archivo `/etc/grub.conf`, como se indica a continuación:

1. Localice las secciones de configuración general en el archivo y agregue las siguientes dos líneas nuevas:

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. Añada dos opciones a la línea del núcleo:

```
kernel ..... console=ttyS1,57600
```

3. Si el archivo `/etc/grub.conf` contiene una directiva `splashimage`, deshabilítela insertando un carácter de comentario.

La [tabla 3-2](#) ofrece un archivo `/etc/grub.conf` de ejemplo que muestra los cambios descritos en este procedimiento.

Tabla 3-2. Archivo de muestra: `/etc/grub.conf`

```
# grub.conf generated by anaconda (grub.conf generado con anaconda)
#
# Note that you do not have to rerun grub after making changes
# to this file
# (Tome en cuenta que no tiene que volver a ejecutar GRUB después de hacer cambios
# en este archivo)
# NOTICE: You do not have a /boot partition. This means that
# all kernel and initrd paths are relative to /, e.g.
# (AVISO: No tiene que una partición /boot. Esto significa que
# todas la rutas de acceso de initrd y kernel se refieren a /, p. ej.,)
# 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/sdal 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/sdal s
initrd /boot/initrd-2.4.9-e.3.im
```

Cuando modifique el archivo `/etc/grub.conf`, siga las siguientes directrices:

1. Desactive la interfaz gráfica de la GRUB y utilice la interfaz a base de texto; de lo contrario, la pantalla de GRUB no se mostrará en la redirección de consola de RAC. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con `splashimage`.
2. Para arrancar varias opciones de GRUB a fin de iniciar sesiones de consola en toda la conexión serie del RAC, agregue la siguiente línea a todas las opciones:

```
console=ttyS1,57600
```

La [tabla 3-2](#) muestra el elemento `console=ttyS1,57600` agregado únicamente en la primera opción.

Permitir Inicio de sesión en la consola después del inicio

Modifique el archivo `/etc/inittab`, como 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 3-3](#) muestra un archivo de ejemplo con la nueva línea.

Tabla 3-3. Archivo de muestra: /etc/inittab

```
#
# inittab This file describes how the INIT process should set up
# the system in a certain run-level.
# (inittab Este archivo describe cómo el proceso INIT debe configurar
# el sistema en un nivel de ejecución determinado.)
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
# (Modificado para RHS Linux por Marc Ewing y Donnie Barnes)
#
# Default runlevel. The runlevels used by RHS are: (Nivel de ejecución
# predeterminado. Los niveles de ejecución utilizados por RHS son:)
# 0 - halt (Do NOT set initdefault to this) (interrumpir [no establezca
# este valor para initdefault])
# 1 - Single user mode (modo de un solo usuario)
# 2 - Multiuser, without NFS (The same as 3, if you do not have
# networking) (varios usuarios, sin NFS [igual que el valor 3,
# si no se tiene conexión de red])
# 3 - Full multiuser mode (modo completo de varios usuarios)
# 4 - unused (sin usar)
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this) (reiniciar
# [no establezca este valor para initdefault])
#
id:3:initdefault:

# System initialization. (Inicialización del sistema.)
si:sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel. (Lo siguiente se debe ejecutar en
# cada nivel de ejecución.)
ud:once:/sbin/update

# Trap CTRL-ALT-DELETE
# (Captura CTRL-ALT-SUPR)
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.
# (Cuando nuestro UPS nos indica que la alimentación falló, digamos que
# tenemos algunos minutos de alimentación restante. Programe un apagado de
# 2 minutos desde este momento.)
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly. (Esto asume, por supuesto,
# que usted tiene la alimentación instalada y que el suministro de alimentación
# ininterrumpida (UPS) está conectado y funciona correctamente.)
pf:powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
# (Si la alimentación se restauró antes de que el apagado entrara en efecto, cáncelo.)
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels (Ejecutar gettys en niveles de ejecución estándar)
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 (Ejecutar xdm en nivel de ejecución 5)
# xdm is now a separate service (xdm es ahora un servicio separado)
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifique el archivo `/etc/securetty`, como se indica a continuación:

Agregue una nueva línea, con el nombre del tty serie para COM2:

```
ttyS1
```

La [tabla 3-4](#) muestra un archivo de ejemplo con la nueva línea.

Tabla 3-4. Archivo de muestra: /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/SSH del DRAC 5

La consola serie, Telnet o SSH puede ser activada de manera local o remota.

Activación de la consola serie/Telnet/SSH del DRAC de manera local

 **NOTA:** Para poder realizar los pasos de esta sección, usted (el usuario actual), 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 desde 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
```

Para obtener información detallada sobre cómo utilizar los comandos de RACADM y serie/Telnet/SSH, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Activación de la consola serie/Telnet/SSH del DRAC de manera remota

Para activar la consola serie/Telnet/SSH de manera remota, escriba los siguientes comandos remotos de RACADM desde una petición de comandos:

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial cfgSerialConsoleEnable 1
```

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial cfgSerialTelnetEnable 1
```

```
racadm -u <nombre de usuario> -p <contraseña> -r <dirección IP del DRAC 5> config -g cfgSerial cfgSerialSshEnable 1
```

Uso del comando RACADM para configurar los valores de la consola Telnet y serie

Este apartado muestra los pasos para configurar los valores de configuración predeterminados para la redirección de consola de serie, Telnet o SSH.

Para configurar los valores, escriba el comando **racadm config** con el grupo, propiedad, y valores de propiedad adecuados para el valor que desea configurar.

Puede escribir comandos RACADM de manera local o remota. Al utilizar comandos RACADM de manera remota, debe incluir el nombre de usuario, la contraseña y la dirección IP del DRAC 5 del sistema administrado.

Para obtener una lista completa de los comandos disponibles de la CLI de RACADM y de la consola serie, Telnet o SSH, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Uso de RACADM de manera local

Para escribir comandos RACADM de manera local, escriba los comandos a continuación desde una petición de comandos en el sistema administrado:

```
racadm config -g <grupo> -o <propiedad> <valor>
```

Para ver una lista de las propiedades, escriba los comandos a continuación desde una petición de comandos en el sistema administrado:

```
racadm getconfig -g <grupo>
```

Uso de RACADM de manera remota

Para utilizar comandos RACADM de manera remota, escriba el comando a continuación desde una petición de comandos en 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 el comando RACADM de manera remota. De lo contrario, RACADM expirará el tiempo de espera y aparecerá el siguiente mensaje:

```
Unable to connect to RAC at specified IP address. (No se puede conectar al RAC en la dirección IP especificada.)
```

Para activar el servidor web por medio de Secure Shell (SSH), Telnet o RACADM local, escriba el siguiente comando en la ventana de símbolo de sistema en una estación de administración:

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

Visualización de valores de configuración

La [tabla 3-5](#) muestra las acciones y comandos relacionados con la consulta de los valores de configuración. Para ejecutar los comandos, abra una ventana de símbolo de sistema en el sistema administrado, escriba el comando y presione <Entrar>.

Tabla 3-5. Visualización de valores de configuración

| Acción | Comando |
|--|---|
| Listar los grupos disponibles. | racadm getconfig -h |
| Mostrar la configuración actual de un grupo particular. | racadm getconfig -g <grupo> Por ejemplo, para mostrar una lista de todos los valores del grupo cfgSerial , escriba el comando siguiente: racadm getconfig -g cfgSerial |
| Mostrar la configuración actual de un grupo particular de manera remota. | racadm -u <usuario> -p <contraseña> -r <dirección IP del DRAC 5> getconfig -g cfgSerial Por ejemplo, para mostrar una lista de todos los valores para el grupo cfgSerial de manera remota, escriba: racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial |

Configuración del número de puerto de Telnet

Escriba el siguiente comando para cambiar el número de puerto de Telnet en el DRAC 5.

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <nuevo número de puerto>
```

Uso de Secure Shell (SSH)

Es crucial que los dispositivos del sistema y la administración de los dispositivos esté segura. Los dispositivos incorporados conectados están en el centro de muchos procesos empresariales. Si estos dispositivos están en riesgo, la empresa del cliente también puede estar en riesgo, lo cual traería nuevas necesidades de seguridad para el software de administración de dispositivos de interfaz de línea de comandos (CLI).

Secure Shell (SSH) es una sesión de línea de comandos que incluye las mismas capacidades que una sesión Telnet, pero con seguridad mejorada. El DRAC 5 admite la versión 2 de SSH con autenticación de contraseña. El SSH se activa en el DRAC 5 cuando usted instala o actualiza el firmware del DRAC 5.

Usted 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 de Secure Shell envía un mensaje de error. El texto del mensaje está en función del cliente y no es controlado por el DRAC 5.

 **NOTA:** OpenSSH se debe ejecutar desde un emulador de terminal ANSI o VT100 en Windows. La ejecución de OpenSSH en la petición de comandos de Windows no producirá una funcionalidad total (es decir, algunas teclas no responderán y no se mostrarán gráficos).

Sólo se admiten cuatro sesiones de SSH en un momento dado. El tiempo de espera de la sesión se controla con la propiedad `cfgSsnMgtSshIdleTimeout`, tal como se describe en la sección "[Definiciones de grupos y objetos de la base de datos de propiedades de DRAC 5](#)".

Usted puede activar el SSH en el DRAC 5 por medio del 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 acerca de las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte "[Definiciones de grupos y objetos de la base de datos de propiedades de DRAC 5](#)".

La implementación de SSH del DRAC 5 es compatible con varios esquemas de cifrado, según se muestra en la [tabla 3-6](#).

Tabla 3-6. Esquemas de cifrado

| Tipo de esquema | Esquema |
|-------------------------|--|
| Criptografía asimétrica | De 512 a 1024 (aleatoriamente) bits de DSA/DSS de Diffie-Hellman de acuerdo a la especificación NIST |
| Criptografía simétrica | <ul style="list-style-type: none"> 1 AES256-CBC 1 RIJNDAEL256-CBC 1 AES192-CBC 1 RIJNDAEL192-CBC 1 AES128-CBC 1 RIJNDAEL128-CBC 1 BLOWFISH-128-CBC 1 3DES-192-CBC 1 ARCFOUR-128 |
| Integridad del mensaje | <ul style="list-style-type: none"> 1 HMAC-SHA1-160 1 HMAC-SHA1-96 1 HMAC-MD5-128 1 HMAC-MD5-96 |
| Autenticación | <ul style="list-style-type: none"> 1 Contraseña |

 **NOTA:** No se admite el SSHv1.

Habilitación de las opciones de seguridad adicionales del DRAC 5

Para prevenir el acceso no autorizado al sistema remoto, el DRAC 5 ofrece las siguientes características:

- 1 Filtración de direcciones IP (IPRange): define un rango específico de las direcciones IP que pueden acceder al DRAC 5.
- 1 Bloqueo de direcciones IP: limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica

En la configuración predeterminada del DRAC 5, estas funciones están desactivadas. Use el siguiente subcomando, o la interfaz basada en web, para activar estas funciones.

```
racadm config -g cfgRacTuning -o <nombre_de_objeto> <valor>
```

Use también estas funciones junto con los valores adecuados de tiempo de espera de sesiones y con un plan definido de seguridad para la red.

Los apartados siguientes proporcionan información adicional sobre estas funciones.

Filtración de IP (IpRange)

La filtración de direcciones IP (o *Comprobación de rango de IP*) permite el acceso al DRAC 5 únicamente a los clientes o estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Todos los demás inicios de sesión serán denegados.

La filtración de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades **cfgRacTuning**:

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

La propiedad **cfgRacTuneIpRangeMask** se aplica tanto a la propiedad de la dirección IP entrante como a la propiedades **cfgRacTuneIpRangeAddr**. Si los resultados de ambas propiedades son idénticos, se permite que la solicitud de inicio de sesión entrante tenga acceso al DRAC 5. Los inicios de sesión provenientes de las direcciones IP que estén fuera de este rango recibirán un mensaje de error.

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

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

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

Consulte "[Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5](#)" para ver una lista completa de propiedades **cfgRacTune**.

Tabla 3-7. Propiedades de filtración de direcciones IP (IpRange)

| Propiedad | Descripción |
|--------------------------------|---|
| cfgRacTuneIpRangeEnable | Activa la función de comprobación del rango de IP. |
| cfgRacTuneIpRangeAddr | <p>Determina el patrón de bits de direcciones IP aceptable, según los unos (1) que haya en la máscara de subred.</p> <p>Esta propiedad se basa en el modo en bits "AND" con cfgRacTuneIpRangeMask para determinar la parte superior de la dirección IP permitida. Cualquier dirección IP que contenga este patrón de bits en los bits superiores tendrá permiso de establecer una sesión en el DRAC 5. Los inicios de sesión que provengan de las direcciones de IP estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten un rango de direcciones de 192.168.1.0 a 192.168.1.255 para establecer una sesión en el DRAC 5.</p> |

| | |
|------------------------------------|--|
| <code>cfgRacTuneIpRangeMask</code> | Define las posiciones de bit significativas en la dirección IP. La máscara de subred debe darse en forma de máscara de red, donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior. |
|------------------------------------|--|

Activación de la filtración de IP

A continuación, se muestra un comando de ejemplo para la configuración de la filtración de IP.

Para obtener más información sobre RACADM y los comandos de RACADM, consulte "[Uso de RACADM](#)".

 **NOTA:** Los siguientes comandos de RACADM bloquean todas las direcciones IP excepto la 192.168.0.57)

Para restringir el inicio de sesión a una sola dirección IP (por ejemplo, 192.168.0.57), utilice la máscara completa, como 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 todos los bits, excepto los dos últimos en la máscara, como se muestra a continuación:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

Directrices de filtración de IP

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

- 1 Asegúrese que `cfgRacTuneIpRangeMask` esté configurada en forma de máscara de red, donde todos bits más significativos son unos (1) (lo que define la subred en la máscara) con una transición total a ceros (0) en los bits del orden inferior.
- 1 Use la dirección base del rango deseado como el valor de `cfgRacTuneIpRangeAddr`. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits del orden inferior en donde la máscara tiene ceros.

Bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el DRAC 5 durante un lapso de tiempo predefinido.

El parámetro de bloqueo de IP usa las funciones del grupo `cfgRacTuning` que incluyen:

- 1 El número de fallas de inicio de sesión permisibles ([cfgRacTuneIpBlkFailcount](#))
- 1 El margen de tiempo en segundos en el que deben presentarse estas fallas ([cfgRacTuneIpBlkFailWindow](#))
- 1 La cantidad de tiempo en segundos durante el que se impide que la dirección IP "culpable" inicie sesión después de haber excedido el número permitido de fallas ([cfgRacTuneIpBlkPenaltyTime](#))

Conforme se acumulan las fallas de inicio de sesión provenientes de una dirección IP específica, un contador interno lleva registro de su antigüedad. Cuando el usuario inicia sesión satisfactoriamente, el historial de fallas se borra y el contador interno se restablece.

 **NOTA:** Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes SSH pueden mostrar el mensaje siguiente: identificación de intercambio de SSH: El host remoto cerró la conexión.

Consulte "[Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5](#)" para ver una lista completa de propiedades `cfgRacTune`.

La [tabla 3-8](#) muestra una lista de los parámetros definidos por el usuario.

Tabla 3-8. Propiedades de restricción de reintentos de inicio de sesión

| Propiedad | Definición |
|--|--|
| <code>cfgRacTuneIpBlkEnable</code> | Activa la función de bloqueo de IP. Cuando se presenten fallas consecutivas (<code>cfgRacTuneIpBlkFailCount</code>) provenientes de una dirección IP determinada dentro de lapso de tiempo específico (<code>cfgRacTuneIpBlkFailWindow</code>), todos los intentos posteriores de establecimiento de sesión que provengan de dicha dirección serán rechazados durante un período de tiempo determinado (<code>cfgRacTuneIpBlkPenaltyTime</code>). |
| <code>cfgRacTuneIpBlkFailCount</code> | Establece el número permitido de fallas de inicio de sesión provenientes de una dirección IP antes de comenzar a rechazar los intentos de inicio de sesión. |
| <code>cfgRacTuneIpBlkFailWindow</code> | El margen de tiempo en segundos dentro del cual se cuentan los intentos fallidos. Cuando las fallas superan este límite, se quitan del contador. |

| | |
|---|---|
| <code>crgRacTuneIpBlkPenaltyTime</code> | Define el lapso de tiempo en segundos durante el cual que se rechazarán todos los intentos de inicio de sesión provenientes de una dirección IP con fallas excesivas. |
|---|---|

Activación del bloqueo de IP

El ejemplo siguiente impide a una dirección IP cliente establecer una sesión durante cinco minutos si dicho cliente ha fallado los cinco intentos de inicio de sesión en un período de un minuto.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente impide que se realicen más de tres intentos fallidos dentro de un minuto e impide más intentos de inicio de sesión durante una hora.

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

Conexión al sistema administrado mediante el puerto serie local o la estación de administración de Telnet (sistema cliente)

El sistema administrado proporciona acceso entre el DRAC 5 y el puerto serie en el sistema para permitirle encender, apagar o restablecer el sistema administrado y acceder a registros.

La consola serie está disponible en el DRAC 5 mediante el conector serie externo del sistema administrado. Sólo un sistema cliente serie (estación de administración) puede estar activo en un momento dado. 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 en un momento dado. La conexión de la estación de administración con la consola serie o Telnet del sistema administrado requiere del software de emulación de terminal de la estación de administración. Consulte "Configuración del software de emulación de terminal de la estación de administración" para obtener más información.

Los siguientes apartados explican cómo conectar la estación de administración al sistema administrado mediante los métodos siguientes:

- 1 Un puerto serie externo del sistema administrado por medio de software de terminal y un cable de módem nulo
- 1 Una conexión Telnet utilizando el software de terminal por medio del NIC del DRAC 5 del sistema administrado o el NIC en modo colaborativo compartido

Conexión del cable DB-9 para la consola serie

Para conectarse al sistema administrado por medio de una consola de texto serie, debe conectar un cable de módem nulo DB-9 al puerto COM del sistema administrado. No todos los cables DB-9 llevan las patas/señales necesarias para esta conexión. El cable DB-9 para esta conexión debe cumplir la especificación mostrada en la [tabla 3-9](#).

 **NOTA:** El cable DB-9 también se puede usar para la redirección de consola de texto del BIOS.

Tabla 3-9. Patas necesarias para el cable de módem nulo DB-9

| Nombre de señal | Pata del DB-9 (pata del servidor) | Pata del DB-9 (pata de la 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 portadora) | 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:

- 1 Linux Minicom en un Xterm
- 1 HyperTerminal Private Edition (versión 6.3) de Hilgraeve
- 1 Linux Telnet en un Xterm
- 1 Microsoft® Telnet

Realice los pasos en los apartados siguientes para configurar el tipo del software de terminal. Si está usando Telnet de Microsoft, no es necesario realizar la configuración.

Configuración de Linux Minicom para emulación de consola serie

Minicom es la utilidad de acceso de puerto serie para 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 de "[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 consola serie

 **NOTA:** Para asegurarse de que el texto se muestra correctamente, Dell recomienda que utilice una ventana Xterm para mostrar la consola Telnet en vez de la consola predeterminada proporcionada por la instalación de Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en la petición de comandos.
2. En la ventana Minicom, mueva la flecha del mouse a la esquina inferior derecha de la ventana y cambie el tamaño a 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 <Minicom nombre de archivo de configuración>` y vaya al [paso 17](#).
4. En la petición de comandos de Xterm, escriba `minicom -s`.
5. Seleccione **Configuración del puerto serie** y pulse <Entrar>.
6. Presione <a> y seleccione el dispositivo serie adecuado (por ejemplo, `/dev/ttyS0`).
7. Pulse <e> y establezca la opción **Bps/Par/Bits** en **57600 8N1**.
8. Pulse <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**, pulse <Entrar>.
10. Seleccione **Módem y marcación** y pulse <Entrar>.
11. En el menú **Marcación de módem y configuración de parámetros**, pulse <Retroceso> para borrar los valores `init`, `reset`, `connect` y `hangup` de modo que queden en blanco.
12. Para guardar cada valor en blanco, presione <Entrar>.
13. Cuando se hayan borrado todos los campos especificados, presione <Entrar> para salir del menú **Marcación de módem y configuración de parámetros**.
14. Seleccione **Guardar configuración como nombre_config** y pulse <Entrar>.
15. Seleccione **Salir de Minicom** y pulse <Entrar>.
16. En la petición del intérprete de comandos, escriba `minicom <Minicom nombre de archivo de configuración>`.
17. Para ampliar la ventana de Minicom a 80 x 25, arrastre la esquina de la misma.
18. Para salir de Minicom, presione <Ctrl+a>, <z>, <x>.

 **NOTA:** Si utiliza Minicom para la redirección de consola de texto serie para configurar el BIOS del sistema administrado, se recomienda que active el color en Minicom. Para activar el color, escriba el siguiente comando en el símbolo del sistema: `minicom -c on`

Asegúrese de que la ventana de Minicom muestra una petición de comandos como [DRAC 5\root]#. Cuando aparezca la petición de comandos, significa que la conexión es correcta y está listo para conectarse a la consola del sistema administrado con el comando serie connect.

Valores de Minicom necesarios para la emulación de consola serie

Utilice la [tabla 3-10](#) para configurar cualquier versión de Minicom.

Tabla 3-10. 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 , reset , connect y hangup de modo que queden en blanco |
| Tamaño de ventana | 80 x 25 (para cambiar el tamaño, arrastre la esquina de la ventana) |

Configuración de HyperTerminal para la 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 de forma adecuada, utilice HyperTerminal Private Edition versión 6.3 de Hilgraeve.

Para configurar HyperTerminal para la redirección de consola serie, realice los pasos siguientes:

1. Inicie el programa HyperTerminal.
2. Escriba un nombre para la nueva conexión y haga clic en **Aceptar**.
3. Junto a **Conectar usando:**, seleccione el puerto COM en la estación de administración (por ejemplo, COM2) a la que ha conectado el cable de módem nulo DB-9 y haga clic en **Aceptar**.
4. Configure los valores del puerto COM como se muestra en la [tabla 3-11](#).
5. Haga clic en **Aceptar**.
6. Haga clic en **Archivo**→ **Propiedades**, y después haga clic en la ficha **Configuración**.
7. Defina la **Id. de la terminal de Telnet:** como **ANSI**.
8. Haga clic en **Configuración de terminal** y establezca **Filas de pantalla** en **26**.
9. Establezca **Columnas** en **80** y haga clic en **Aceptar**.

Tabla 3-11. Valores del puerto COM de la estación de administración

| Descripción del valor | Valor necesario |
|-----------------------|-----------------|
| Bits por segundo | 57600 |
| Bits de datos | 8 |
| Paridad | Ninguna |
| Bits de paro | 1 |
| Control de flujo | Hardware |

La ventana de HyperTerminal muestra una petición de comandos como [DRAC 5\root]#. Cuando aparezca la petición de comandos, significa que la conexión es correcta y está listo para conectarse a la consola del sistema administrado con el comando serie connect com2.

Configuración de Linux XTerm para la redirección de la consola Telnet

Siga las directrices a continuación cuando realice los pasos en esta sección:

1. 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.

1. Para asegurarse de que el texto se muestra correctamente, Dell recomienda que utilice una ventana Xterm para mostrar la consola Telnet en vez de la consola predeterminada proporcionada por la instalación de Linux.

Para ejecutar Telnet con Linux, realice los pasos a continuación:

1. Inicie una nueva sesión de Xterm.

En la ventana de símbolo de sistema, 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 de Microsoft no muestren la pantalla de configuración del BIOS correctamente cuando se establece la redirección de consola de BIOS como emulación VT100. Si se presenta este problema, actualice la pantalla cambiando la redirección de consola de BIOS al modo ANSI. 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.
3. Abra una petición de comandos, escriba lo siguiente y presione <Entrar>:

```
telnet <dirección IP>:<número de puerto>
```

donde *número de puerto* es la dirección IP del DRAC 5 y *número de puerto* es el número del puerto Telnet (si está usando un nuevo puerto).

Configuración de la tecla de retroceso para la sesión Telnet

Dependiendo del cliente Telnet, al presionar la tecla <Retroceso> puede obtener resultados inesperados. Por ejemplo, la sesión puede mostrar ^h. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux se pueden configurar para usar la tecla <Retroceso>.

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

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

```
telnet
```

Si ya tiene una sesión Telnet abierta, presione <Ctrl><]>.

3. En la petición, escriba:

```
set bsasdel
```

Aparecerá el siguiente mensaje:

```
Backspace will be sent as delete.
```

(La tecla de retroceso se enviará como "suprimir".)

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

1. Abra una ventana de símbolo de sistema y escriba:

```
stty erase ^h
```

2. En la petición, escriba:

```
telnet
```

Uso de una consola Telnet o serie

Los comandos **serial** y **telnet** y la CLI de RACADM pueden escribirse en una consola serie o Telnet y ejecutarse en el servidor de manera local o remota. La CLI de RACADM local se instala para uso exclusivo de un usuario root.

Para obtener más información sobre los comandos de serie, Telnet o SSH y de la CLI de RACADM, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Cómo ejecutar Telnet con Windows XP o Windows 2003

Si la estación de administración está ejecutando Windows XP o Windows 2003, es posible que tenga un problema con los caracteres en las sesiones Telnet del DRAC 5. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla <Entrar> no responde y no aparece la petición de contraseña.

Para resolver este problema, descargue la revisión 824810 del sitio web de asistencia de Microsoft en support.microsoft.com. Para obtener más información, consulte el artículo 824810 de Microsoft Knowledge Base.

Cómo ejecutar Telnet con Windows 2000

Si la estación de administración está ejecutando Windows 2000, no podrá ingresar al programa de configuración del BIOS presionando la tecla <F2>. Para resolver este problema, use el cliente Telnet incluido en la descarga gratuita recomendada de los servicios de Windows para UNIX@ 3.5 de Microsoft. Usted puede descargar los servicios de Windows para UNIX 3.5 del sitio www.microsoft.com/windows/sfu/downloads/default.asp.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración del DRAC 5 por medio de la interfaz de usuario basada en web

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Acceso a la interfaz basada en web](#)
- [Configuración del NIC del DRAC 5](#)
- [Adición y configuración de usuarios del DRAC 5](#)
- [Configuración y administración de los certificados de Active Directory](#)
- [Cómo asegurar las comunicaciones del DRAC 5 por medio de certificados SSL y digitales](#)
- [Configuración de los modos de serie y de terminal](#)
- [Configuración de la comunicación serie en la LAN](#)
- [Configuración de servicios](#)
- [Preguntas frecuentes](#)

El DRAC 5 proporciona una interfaz basada en 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 diaria de sistemas, utilice la interfaz basada en web del DRAC 5. Este capítulo proporciona información sobre cómo realizar tareas comunes de administración de sistemas con la interfaz basada en web del DRAC 5 y proporciona vínculos a la información relacionada.

Todas las tareas de configuración de la interfaz basada en web también se pueden realizar con RACADM. Para obtener una lista de todos los comandos de la consola serie/Telnet/SSH y de RACADM que se pueden utilizar para realizar equivalentes de texto de cada tarea, consulte "[Uso de la interfaz de línea de comandos de RACADM](#)".

Consulte la ayuda en línea del DRAC 5 para buscar información de contextos relacionados acerca de cada página de la interfaz basada en web.

Acceso a la interfaz basada en web

Para acceder a la interfaz basada en web del DRAC 5, realice los pasos a continuación:

1. Abra una ventana de un explorador compatible de web.

Para obtener más información, consulte "[Exploradores de web admitidos](#)".

2. En el campo **Dirección**, escriba lo siguiente y presione <Entrar>:

```
https://<dirección IP>
```

Si se ha cambiado el número predeterminado del 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* es el número del puerto HTTPS.

Aparece la ventana **Conectar** del DRAC 5.

Conexión

Puede iniciar sesión como usuario del DRAC 5 o como usuario de Microsoft® Active Directory®. El nombre de usuario y la contraseña predeterminados son **root** y **calvin**, respectivamente.

Antes de iniciar sesión en el DRAC 5, compruebe que cuenta con permiso para **Iniciar sesión en el DRAC 5**.

Para conectar, realice los pasos siguientes:

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

- 1 Su nombre de usuario del 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

- 1 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 \john_doe** o **john_doe@dell.com**.

El campo de nombre de usuario de Active Directory no distingue entre mayúsculas y minúsculas.

2. En el campo **Contraseña**, escriba su contraseña de usuario del DRAC 5 o su contraseña de usuario de Active Directory.

Este campo distingue mayúsculas y minúsculas.

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

Desconexión

1. En la esquina superior derecha de ventana de la interfaz basada en web del DRAC 5, haga clic en **Desconectar** para cerrar la sesión.
2. Cierre la ventana del explorador.

 **NOTA:** El botón **Desconectar** no aparecerá sino hasta que usted haya iniciado sesión.

 **NOTA:** El cierre del explorador sin una desconexión ordenada ocasiona que la sesión permanezca abierta hasta que se acabe el tiempo de espera. Se recomienda enfáticamente que haga clic en el botón de desconectar para terminar la sesión; de lo contrario, la sesión permanecerá activa hasta que se acabe el tiempo de espera de la sesión.

Configuración del NIC del DRAC 5

Configuración de la red y los valores de la LAN de IPMI

 **NOTA:** Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el DRAC 5**.

 **NOTA:** La mayoría de los servidores DHCP requieren que un servidor almacene un símbolo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el DRAC 5) debe proporcionar este símbolo durante la negociación de DHCP. Para los RAC, el DRAC 5 proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

 **NOTA:** Si el DRAC del sistema administrado está configurado en modo **Compartido** o **Compartido con protección contra fallas** y el DRAC está conectado a un conmutador con el Protocolo de árbol de distribución (STP) activado, los clientes de la red experimentarán un retraso de 20 a 30 segundos en la conexión cuando el estado de la conexión LOM de la estación de administración cambie durante la convergencia de STP.

1. En el árbol de **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Red**.
3. En la página **Configuración de la red**, configure los valores del NIC del DRAC 5.
La [tabla 4-1](#) y la [tabla 4-2](#) describen la **Configuración de la red** y la **Configuración de IPMI** en la página **Configuración de la red**.
4. Cuando termine, haga clic en **Aplicar cambios**.
5. Para continuar, haga clic en el botón adecuado de la página **Configuración de la red**. Consulte la [tabla 4-3](#).

Tabla 4-1. Configuración de la red

| Valor | Descripción |
|---|---|
| Selección de NIC | Muestra el modo del NIC seleccionado (Dedicado , Compartido con protección contra fallas o Compartido). El valor predeterminado es Dedicado . |
| Dirección MAC | Muestra la dirección MAC del DRAC 5. |
| Activar el NIC | Active el NIC del DRAC 5 y los controles restantes en este grupo. El valor predeterminado es Activado . |
| Usar DHCP (para la dirección IP del NIC) | Permite que Dell OpenManage™ Server Administrator obtenga la dirección IP del DRAC 5 a partir del servidor de Protocolo de configuración dinámica de host (DHCP). Si selecciona esta casilla desactivará los controles Dirección IP estática , Puerta de enlace estática y Máscara de subred estática . El valor predeterminado es Desactivado . |
| Dirección IP estática | Especifica o edita la dirección IP estática para el NIC del DRAC 5. Para cambiar este valor, deseleccione la casilla de marcación Usar DHCP (para dirección IP del NIC) . |
| Puerta de enlace estática | Especifica o edita la puerta de enlace estática para el NIC del DRAC 5. Para cambiar este valor, deseleccione la casilla de marcación Usar DHCP (para dirección IP del NIC) . |
| Máscara de subred estática | Especifica o edita la máscara de subred estática para el NIC del DRAC 5. Para cambiar este valor, deseleccione la casilla de marcación Usar DHCP (para dirección IP del NIC) . |
| Usar DHCP para obtener direcciones de servidor DNS | Obtiene las direcciones del servidor DNS primaria y secundaria a partir del servidor DHCP en vez de usar la configuración estática. El valor predeterminado es Desactivado . |
| Servidor DNS preferido estático | Utiliza la dirección IP del servidor DNS primario solamente cuando no está seleccionada la opción Usar DHCP para obtener las direcciones del servidor DNS . |

| | |
|--|---|
| Servidor DNS alternativo estático | Utiliza la dirección IP del servidor DNS secundario solamente cuando no está seleccionada la opción Usar DHCP para obtener las direcciones del servidor DNS. Puede introducir la dirección IP 0.0.0.0 si no cuenta con un servidor DNS alternativo. |
| Registrar el DRAC en DNS | Registra el nombre del DRAC 5 en el servidor DNS. El valor predeterminado es Desactivado . |
| Nombre DNS del DRAC | Muestra el nombre del DRAC 5 sólo cuando se selecciona Registrar DRAC 5 en el DNS . El nombre de DRAC 5 predeterminado es <i>RAC-etiqueta de servicio</i> , donde <i>etiqueta de servicio</i> 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 del dominio DNS predeterminado. Cuando la casilla no está seleccionada y la opción Registrar DRAC 5 en el DNS está seleccionada, puede modificar el nombre del dominio DNS en el campo Nombre del dominio DNS. El valor predeterminado es Desactivado . |
| Nombre del Dominio DNS | El nombre del dominio DNS predeterminado es MYDOMAIN . Cuando la casilla de marcación Usar DHCP para el nombre del dominio DNS está seleccionada, esta opción estará deshabilitada y usted no 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 establezca el Modo dúplex y la Velocidad de red manualmente (Desactivado). |
| Velocidad de red | Establece la velocidad de red a 100 Mb o 10 Mb para coincidir con su entorno de red. Esta opción no está disponible si Negociar automáticamente se ha establecido en Activado . |
| Modo dúplex | Establece el modo dúplex como completo o semidúplex para coincidir con su entorno de red. Esta opción no está disponible si Negociar automáticamente se ha establecido en Activado . |

Tabla 4-2. Configuración de la LAN IPMI

| Valor | Descripción |
|--|--|
| Activar IPMI en la LAN | Activa el canal de LAN de IPMI. |
| Límite de nivel de privilegio del canal | Configura el nivel máximo de privilegio del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: administrador, operador o usuario. |
| Clave de cifrado | Configura el formato de carácter de la clave de cifrado: de 0 a 20 caracteres hexadecimales (no se permiten espacios). El valor predeterminado es 00000000000000000000. |
| Activar identificación de VLAN | Activa la identificación de VLAN. Si está activada, sólo se aceptará el tráfico de identificación de VLAN que coincida. |
| Identificación de VLAN | El campo de identificación de VLAN de campos 802.1g. |
| Prioridad | El campo de prioridad de campos 802.1g. |

Tabla 4-3. Botones de la página de configuración de la red

| Botón | Descripción |
|-------------------------------|---|
| Imprimir | Imprime la página Configuración de red . |
| Actualizar | Recarga la página Configuración de red . |
| Configuración avanzada | Muestra la página Seguridad de la red . |
| Aplicar cambios | Guarda los cambios realizados en la configuración de red. NOTA: Los cambios de configuración de la dirección IP del NIC cerrarán todas las sesiones de usuario y requerirán que los usuarios se vuelvan a conectar a la interfaz basada en web del DRAC 5 con los valores actualizados de la dirección IP. Todos los demás cambios requerirán que se restablezca el NIC, lo que puede ocasionar una breve pérdida de la conectividad. |

Configuración de los valores de seguridad de la red

 **NOTA:** Para poder realizar los pasos a continuación, se debe tener permiso para **Configurar el DRAC 5**.

1. En el árbol de Sistema, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Red**.
3. En la página de **Configuración de red**, haga clic en **Configuración avanzada**.
4. En la página **Seguridad de la red**, configure los valores de los atributos y luego haga clic en **Aplicar cambios**.

La [tabla 4-4](#) 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 4-5](#).

Tabla 4-4. Configuración de la página de seguridad

| Configuración | Descripción |
|---|--|
| Rango IP activado | Activa la función de comprobación del rango de IP, la cual define un rango específico de las direcciones IP que pueden acceder al DRAC 5. |
| Dirección de rango IP | Determina la dirección aceptable de subred IP. |
| Máscara de subred de rango IP | Define las posiciones de bit significativas en la dirección IP. La máscara de subred debe darse en forma de máscara de red, donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior. Por ejemplo: 255.255.255.0 |
| Bloqueo de IP activado | Activa la función de bloqueo de dirección IP, la cual limita el número de intentos de inicio de sesión fallidos provenientes de una dirección IP específica dentro de un período previamente seleccionado. |
| Número de fallos de bloqueo de IP | Establece el número de intentos fallidos de inicio de sesión provenientes de la misma dirección IP que se admitirán antes de comenzar a rechazar los intentos de inicio de sesión que provengan de dicha dirección. |
| Ventana de fallos de bloqueo de IP | Determina el período en segundos dentro de cual deben ocurrir los incrementos al número de fallas para bloqueo de IP a fin de dar inicio al tiempo de penalización de bloqueo de IP. |
| Tiempo de penalización de bloqueo de IP | El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. |

Tabla 4-5. Botones de la página de seguridad

| 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 realizados en la página Seguridad de la red. |
| Volver a la página de configuración de la red | Regresa a la página Configuración de la red. |

Adición y configuración de 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 con *autoridad basada en funciones*). Para obtener una mayor seguridad, también puede configurar alertas que se envíen por correo electrónico a usuarios específicos cuando se presenten sucesos específicos del sistema.

Para agregar y configurar los usuarios del DRAC 5, realice los pasos a continuación:

 **NOTA:** Para poder realizar los pasos a continuación, se debe tener permiso para configurar el DRAC 5.

1. Expanda el árbol de **Sistema**, 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**, el **Privilegio del RAC**, el **Privilegio de LAN de IPMI** y el **Privilegio de la conexión serie de IPMI** de cada usuario.

3. En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.
4. En la página **Configuración de usuario**, configure las propiedades y los privilegios del usuario.

La [tabla 4-6](#) describe los valores **Generales** para configurar un nombre de usuario o una contraseña del DRAC nuevos o existentes.

La [tabla 4-7](#) describe los **Privilegios del usuario de IPMI** para configurar los privilegios de LAN del usuario.

La [tabla 4-8](#) describe los **Permisos del grupo de usuarios** para la configuración de los **Privilegios del usuario de IPMI** y los **Privilegios de usuario del DRAC**.

La [tabla 4-9](#) describe las listas de los permisos del **Grupo de DRAC**. Si agrega un privilegio de usuario del DRAC al grupo de administrador, usuario avanzado o usuario invitado, el **Grupo de DRAC** cambiará a grupo **Personalizado**.

5. Cuando termine, haga clic en **Aplicar cambios**.
6. Para continuar, haga clic en el botón adecuado de la página **Configuración de usuario**. Consulte la [tabla 4-10](#).

Tabla 4-6. Propiedades generales

| Propiedad | Descripción |
|-----------|-------------|
|-----------|-------------|

| | |
|-----------------------------------|---|
| Identificación de usuario | Especifica uno de los 16 números preconfigurados de identificación de usuario. Si está editando la información del usuario "root", este campo es estático. No se puede modificar el nombre de usuario de "root". |
| Activar el usuario | Habilita al usuario para que pueda acceder al DRAC 5. Cuando está deseleccionada, no se puede cambiar el nombre de usuario. |
| Nombre del usuario | Especifica un nombre de usuario del DRAC 5 de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único. NOTA: Los nombres de usuario del DRAC 5 local no pueden incluir la / (diagonal) ni el . (punto). NOTA: Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el próximo inicio de sesión del mismo. |
| Cambiar contraseña | Activa los campos Contraseña nueva y Confirmar contraseña nueva . Cuando está deseleccionada, no se puede cambiar la Contraseña del usuario. |
| 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 4-7. Privilegios del usuario de IPMI

| Propiedad | Descripción |
|---|---|
| Privilegio máximo permitido de usuario de LAN | Especifica el privilegio máximo del usuario en el canal de LAN de IPMI como uno de los siguientes grupos de usuario: 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 como 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. Cuando está seleccionada, este privilegio está activado. |

Tabla 4-8. Privilegios de usuario del DRAC

| Propiedad | Descripción |
|--|--|
| Grupo de DRAC | Especifica el privilegio máximo de del usuario del DRAC como uno de los siguientes: Administrador , Usuario avanzado , Usuario invitado , Ninguno o Personalizado . Consulte la tabla 4-9 para ver los permisos del Grupo de DRAC . |
| Iniciar sesión en el DRAC | Permite al usuario iniciar sesión en el DRAC. |
| Configurar el DRAC | Permite al usuario configurar el DRAC. |
| Configurar usuarios | Permite al usuario determinar los usuarios específicos que tendrán acceso al sistema. |
| Borrar registros | Permite al usuario borrar los registros del DRAC. |
| Ejecutar comandos de control del servidor | Permite al usuario ejecutar comandos de racadm. |
| Acceder a redirección de consola | Permite al usuario ejecutar la redirección de consola. |
| Acceder a los medios virtuales | Permite al usuario ejecutar y usar los medios virtuales. |
| Probar alertas | Permite al usuario enviar alertas de prueba (mensajes de correo electrónico y capturas de sucesos de plataforma) a un usuario específico. |
| Ejecutar comandos de diagnóstico | Permite al usuario ejecutar comandos de diagnóstico. |

Tabla 4-9. Permisos del grupo de DRAC

| Grupo de usuarios | Permisos concedidos |
|-------------------------|---|
| Administrador | Iniciar sesión en el DRAC 5 , Configurar el DRAC 5 , Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la redirección de consola , Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico |
| Usuario avanzado | Iniciar sesión en el DRAC 5 , Borrar registros, Ejecutar comandos de control del servidor, Acceder a la redirección de consola , Acceder a los medios virtuales, Probar alertas |
| Usuario invitado | Iniciar sesión en el DRAC 5 |
| Personalizado | Selecciona cualquier combinación de los permisos siguientes: Iniciar sesión en el DRAC 5 , Configurar el DRAC 5 , Configurar usuarios, Borrar registros, Ejecutar comandos de acción del servidor , Acceder a la redirección de consola , Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico |
| Ninguna | Sin permisos asignados |

Tabla 4-10. Botones de la página de configuración de usuarios

| | |
|--|--|
| | |
|--|--|

| Botón | Acción |
|--------------------------------|---|
| Imprimir | Imprime la página Configuración de usuario |
| Actualizar | Vuelve a cargar la página Configuración de usuario |
| Volver a la página de usuarios | Regresa a la Página de usuarios . |
| Aplicar cambios | Guarda los cambios realizados en la configuración de red. |

Configuración y administración de los certificados de Active Directory

 **NOTA:** Debe tener permiso para **Configurar el DRAC 5** para configurar Active Directory y para cargar, descargar y ver un certificado de Active Directory.

Use el servicio Microsoft® Active Directory® para configurar el software a fin de proporcionar el acceso al DRAC 5. El servicio le permite agregar y controlar los privilegios de los usuarios existentes del DRAC5.

Para obtener más información, consulte "[Uso del DRAC 5 con Microsoft Active Directory](#)".

Para acceder al menú principal de Active Directory:

1. Expanda el árbol de **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y haga clic en **Active Directory**.

La [tabla 4-11](#) muestra una lista de las opciones de la página **Menú principal de Active Directory**. Los botones de la [tabla 4-12](#) están disponibles en la página **Menú principal de Active Directory**.

Tabla 4-11. Opciones de la página de menú principal de Active Directory

| Campo | Descripción |
|--|--|
| Configurar Active Directory | Configura los valores del nombre del DRAC de Active Directory, el nombre del dominio raíz, el nombre del dominio de DRAC y el tiempo de espera de autenticación de Active Directory. |
| Cargar certificado de CA de Active Directory | Carga un certificado de Active Directory al DRAC. |
| Descargar certificado de servidor del DRAC | El administrador de descargas de Windows le permite descargar un certificado de servidor de DRAC en el sistema. |
| Ver certificado de CA de Active Directory | Muestra el certificado de Active Directory que ha sido cargado en el DRAC. |

Tabla 4-12. Botones de la página de menú principal de Active Directory

| Botón | Definición |
|-----------|--|
| Imprimir | Imprime el contenido de la ventana abierta en la impresora predeterminada. |
| Siguiente | Pasa a la siguiente página seleccionada de Opción . |

Configuración de Active Directory

1. En la página **Menú principal de Active Directory**, seleccione **Configurar Active Directory** y haga clic en **Siguiente**.
2. En la página **Configuración de Active Directory**, introduzca los valores para Active Directory.
La [tabla 4-13](#) describe los valores de la página **Configuración de Active Directory**.
3. Haga clic en **Aplicar** para guardar los valores.
4. Para continuar, haga clic en el botón adecuado de la página **Configuración de Active Directory**. Consulte la [tabla 4-14](#).

Tabla 4-13. Valores de la página de configuración de Active Directory

| Valor | Descripción |
|----------------------------|---|
| Habilitar Active Directory | Activa el Active Directory. Seleccionado = activado; deseleccionado = desactivado |
| Nombre del DRAC | El nombre que identifica de manera exclusiva a la tarjeta DRAC 5 en Active Directory. De manera predeterminada, este valor es NULO. |

| | |
|------------------------------------|--|
| | El nombre debe ser una cadena de 1 a 256 caracteres ASCII, sin espacios en blanco entre ellos. |
| Nombre del dominio raíz | El nombre del dominio raíz de Active Directory. De manera predeterminada, este valor es NULO. El nombre debe ser un nombre de dominio válido que consista de x.y, donde "x" es una cadena de 1 a 256 caracteres ASCII sin espacios en blanco entre ellos y "y" es un tipo de dominio válido como com, edu, gov, int, mil, red, org. |
| Nombre del dominio del DRAC | El nombre DNS (cadena) del dominio donde reside el objeto DRAC 5 de Active Directory. De manera predeterminada, este valor es NULO. El nombre debe ser un nombre de dominio válido que consista de x.y, donde "x" es una cadena de 1 a 256 caracteres ASCII sin espacios en blanco entre ellos y "y" es un tipo de dominio válido como com, edu, gov, int, mil, red, org. |
| Tiempo de espera | El tiempo de espera en segundos para que se completen las consultas de Active Directory. El valor mínimo es más de 15 segundos. El valor predeterminado es de 120 segundos. |

Tabla 4-14. Botones de la página de configuración de Active Directory

| Botón | Descripción |
|--|--|
| Imprimir | Imprime la página Configuración de Active Directory . |
| Aplicar | Guarda los cambios que se realizaron en la página Configuración de Active Directory . |
| Volver al menú principal de Active Directory | Regresa a la página Menú principal de Active Directory . |

Cómo cargar un certificado de CA de Active Directory

1. En la página **Menú principal de Active Directory**, seleccione **Cargar certificado de CA de Active Directory** y haga clic en **Siguiente**.
2. En la página **Carga del certificado**, en el campo **Ruta de acceso del archivo**, escriba la ruta de acceso del archivo de certificado o haga clic en **Examinar** para desplazarse al archivo de certificado.

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

3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón adecuado de la página **Carga del certificado**. Consulte la [tabla 4-15](#).

Tabla 4-15. Botones de la página de carga de certificados

| Botón | Descripción |
|--|---|
| Imprimir | Imprime la página Carga del certificado . |
| Volver al menú principal de Active Directory | Regresa a la página Menú principal de Active Directory . |
| Aplicar | Aplica el certificado al firmware del DRAC 5. |

Cómo descargar un certificado de servidor del DRAC

1. En la página **Menú principal de Active Directory**, seleccione **Descargar certificado de servidor del 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

Use la página **Menú principal de Active Directory** para ver un 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 4-16](#) describe los campos y descripciones asociadas que se listan en la ventana **Certificado**.
La [tabla 4-17](#) describe los botones disponibles en la página **Ver certificado de CA de Active Directory**.
2. Para continuar, haga clic en el botón adecuado de la página **Ver certificado de CA de Active Directory**. Consulte la [tabla 4-17](#).

Tabla 4-16. Información del certificado de CA de Active Directory

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

Tabla 4-17. Botones de la página Ver certificado de CA de Active Directory

| Botón | Descripción |
|--|---|
| Imprimir | Imprime el Certificado de CA de Active Directory. |
| Volver al menú principal de Active Directory | Regresa a la página Menú principal de Active Directory. |

Cómo asegurar las comunicaciones del DRAC 5 por medio de certificados SSL y digitales

Este apartado ofrece información sobre las funciones de seguridad de datos siguientes que vienen incorporadas en el DRAC 5:

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

Capa de conexión segura (SSL)

El DRAC incluye a un servidor de web que está configurado para usar el protocolo de seguridad SSL, que es el estándar en la industria, para transferir por Internet la fecha cifrada. Como está cimentado en la tecnología de cifrado de claves privada y pública, la SSL es una técnica ampliamente aceptada para proporcionar comunicación cifrada y autenticada entre clientes y servidores a fin de prevenir el espionaje en una red.

La SSL permite un sistema habilitado con ésta característica realice las siguientes tareas:

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

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

El servidor de web del DRAC incluye un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar la alta seguridad en la Internet, sustituya el certificado SSL del servidor web mediante el envío de una 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 un obtener un certificado de servidor seguro. Los certificados de servidor seguro garantizan la identidad de un sistema remoto y se aseguran de que la información intercambiada con el sistema remoto no pueda ser vista ni modificada por otros. Para garantizar la seguridad del DRAC, se recomienda enfáticamente que genere una CSR, envíe la CSR a una autoridad de certificados y cargue el certificado que reciba de la autoridad de certificados.

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

Una vez que la CA aprueba la CSR y le envía un certificado, usted debe cargarlo 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.

Cómo acceder al menú principal de SSL

1. Expanda el árbol de Sistema, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **SSL**.

Use las opciones de la página **Menú principal de SSL** (consulte la [tabla 4-18](#)) para generar una CSR para enviarla a una autoridad de certificados. La información de la CSR se almacena en el firmware del DRAC 5. Los botones de la [tabla 4-19](#) están disponibles en la página **Menú principal de SSL**.

Tabla 4-18. 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 sobrescribirá la CSR anterior en el firmware. Para que una CA acepte su CSR, la CSR del firmware debe coincidir con el certificado devuelto por la CA. |
| Cargar certificado del servidor | Haga clic en Siguiente para cargar un certificado existente sobre el que su compañía tiene derechos y utiliza para controlar el acceso al DRAC 5. AVISO: El DRAC 5 sólo acepta los certificados codificados base 64, X509. No se aceptan los certificados codificados DER. Cargue un nuevo certificado para sustituir el certificado predeterminado que recibió con su DRAC 5. |
| Ver certificado del servidor | Haga clic en Siguiente para ver un certificado del servidor existente. |

Tabla 4-19. Botones del menú principal de SSL

| Botón | Descripción |
|-----------|--|
| Imprimir | Imprime la página Menú principal de SSL . |
| Siguiente | Pasa a la siguiente página. |

Generación de una nueva solicitud de firma de certificado

 **NOTA:** Cada nueva CSR sobrescribirá la CSR anterior en el firmware. Antes de que una autoridad de certificados pueda aceptar su CSR, la CSR en el firmware debe coincidir con el certificado devuelto por la autoridad de certificados. 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 valor de atributo de la CSR.

La [tabla 4-20](#) 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. Para continuar, haga clic en el botón adecuado de la página **Generar solicitud de firma de certificado (CSR)**. Consulte la [tabla 4-21](#).

Tabla 4-20. Opciones de la página de generación de solicitud de firma de certificados (CSR)

| Campo | Descripción |
|----------------------------------|---|
| Nombre común | El nombre exacto que se certifica (por lo general el nombre del dominio del Web Server, por ejemplo, www.empresa-xyz.com). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos. |
| Nombre de la organización | El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios. |
| Unidad de organización | El nombre asociado con una unidad de organización, como un departamento (por ejemplo, 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 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 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 4-21. Botones de la página de generación de solicitud de firma de certificados (CSR)

| Botón | Descripción |
|--|---|
| Imprimir | Imprime la página Generar solicitud de firma de certificados (CSR). |
| Volver al menú principal de seguridad | Regresa a la página Menú principal de SSL . |
| Generar | Genera una CSR. |

Carga de un certificado del servidor

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

Aparecerá la página **Carga del certificado**.

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

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

3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón adecuado de la página. Consulte la [tabla 4-22](#).

Tabla 4-22. Botones de la página de carga de certificados

| Botón | Descripción |
|--|--|
| Imprimir | Imprime la página Carga del certificado. |
| Volver al menú principal de SSL | Regresa a la página Menú principal de SSL . |
| Aplicar | Aplica el certificado al firmware del DRAC 5. |

Visualización de un certificado del servidor

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

La [tabla 4-23](#) describe los campos y descripciones asociadas que se listan en la ventana **Certificado**.

2. Para continuar, haga clic en el botón adecuado de la página **Ver certificado del servidor**. Consulte la [tabla 4-24](#).

Tabla 4-23. Información del certificado

| Campo | Descripción |
|--------------------------------|--|
| Número de serie | Número serie del certificado |
| Información del titular | Atributos del certificado introducidos por el asunto |
| Información del emisor | Atributos del certificado devueltos por el emisor |
| Válido desde | Fecha de emisión del certificado |
| Válido hasta | Fecha de caducidad del certificado |

Tabla 4-24. Botones de página de visualización de certificados del servidor

| Botón | Descripción |
|--|--|
| Imprimir | Imprime la página Ver certificado del servidor. |
| Volver al menú principal de SSL | Regresa a la página Menú principal de SSL . |

Configuración de los modos de serie y de terminal

Configuración de las conexiones serie de IPMI y de RAC

1. Expande el árbol de Sistema, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
3. Configure los valores de la conexión serie de IPMI.
La [tabla 4-25](#) ofrece información acerca de la configuración de la conexión serie de IPMI.
4. Configure los valores de la conexión serie del RAC.
La [tabla 4-26](#) ofrece información acerca de la configuración de la conexión serie del RAC.
5. Haga clic en **Aplicar cambios**.
6. Para continuar, haga clic en el botón adecuado de la página **Configuración de la conexión serie**. Consulte la [tabla 4-27](#).

Tabla 4-25. Valores de la conexión serie de IPMI

| Valor | Descripción |
|--|--|
| Configuración del modo de conexión | <ul style="list-style-type: none"> 1 Modo básico de conexión directa: modo básico de la conexión serie de IPMI 1 Modo de terminal de conexión directa: modo de terminal de la conexión serie de IPMI |
| Velocidad en baudios | Establece la velocidad en baudios. Seleccione 9600 bps , 19,2 kbps , 57,6 kbps o 115,2 kbps . |
| Control de flujo | <ul style="list-style-type: none"> 1 Ninguno: control de flujo de hardware desactivado 1 RTS/CTS: control de flujo de hardware activado |
| Límite de nivel de privilegio del canal | <ul style="list-style-type: none"> 1 Administrador 1 Operador 1 Usuario |

Tabla 4-26. Valores de la conexión serie del RAC

| Valor | Descripción |
|-------------------------------------|---|
| Activado | Activa o desactiva la de consola serie del RAC. Seleccionado = activada; deseleccionado = desactivada |
| Máximo de sesiones | El número máximo de sesiones simultáneas que se permiten para este sistema. |
| Tiempo de espera | La cantidad máxima de segundos que la línea permanece disponible antes de desconectarse. El rango es de 60 a 1920 segundos. El valor predeterminado es de 300 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. |
| Redireccionamiento activado | Activa o desactiva la redirección de consola. Seleccionado = activado; deseleccionado = desactivado |
| Velocidad en baudios | La velocidad de los datos en el puerto serie externo. Seleccione 9600 bps , 28,8 kbps , 57,6 kbps y 115,2 kbps . El valor predeterminado es 57,6 kbps . |
| Tecla Esc | Especifica la tecla <Esc>. El valor predeterminado son los caracteres ^\. |
| Tamaño de búfer de historial | El tamaño del búfer de historial de la conexión serie, el cual guarda los últimos caracteres que fueron escritos en la consola. El valor máximo y predeterminado es de 8192 caracteres. |
| Comando de inicio de sesión | La línea de comandos del DRAC que se debe ejecutar ante un inicio de sesión válido. |

Tabla 4-27. 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 IPMI y del RAC. |
| Configuración del modo de terminal | Abre la página Configuración del modo de terminal . |

Configuración del modo de terminal

1. Expande el árbol de Sistema, haga clic en **Acceso remoto**.

- Haga clic en la ficha **Configuración** y después haga clic en **Serie**.
- En la página de **Configuración de la conexión serie**, haga clic en **Configuración del modo de terminal**.
- Configure los valores del modo de terminal.

La [tabla 4-28](#) ofrece información acerca de la configuración del modo de terminal.

- Haga clic en **Aplicar cambios**.
- Para continuar, haga clic en el botón adecuado de la página **Configuración del modo de terminal**. Consulte la [tabla 4-29](#).

Tabla 4-28. Configuración del modo de terminal

| Valor | Descripción |
|--|---|
| Edición de línea | Activa o desactiva la edición de línea. |
| Control de eliminación | Selecciona uno de los siguientes valores: <ul style="list-style-type: none"> 1 El BMC genera un carácter <retroceso><espacio><retroceso> cuando se recibe un <retroceso> o <supr> 1 El BMC genera un carácter <supr> cuando se recibe un <retroceso> o <supr> |
| Control del eco | Activa o desactiva el eco. |
| Control del protocolo de enlace | Activa o desactiva el protocolo de establecimiento de conexión. |
| Nueva secuencia de línea | Seleccione Ninguna, <retorno de carro, salto de línea>, <NULO>, <retorno de carro>, <salto de línea, retorno de carro> o <salto de línea>. |
| Introducir una nueva secuencia de línea | Seleccione <retorno de carro> o <NULO>. |

Tabla 4-29. 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 . |
| Volver a la configuración del puerto serie | Regresa a la página Configuración del puerto serie . |
| Aplicar cambios | Aplica los cambios de la configuración del modo de terminal. |

Configuración de la comunicación en serie en la LAN

 **NOTA:** Para obtener información completa sobre la comunicación en serie en la LAN, consulte la *Guía del usuario del controlador de administración de la placa base de Dell OpenManage*.

- Expanda el árbol de **Sistema**, haga clic en **Acceso remoto**.
- Haga clic en la ficha **Configuración** y después haga clic en **Comunicación en serie en la LAN**.
- Configure los valores de la comunicación en serie en la LAN.

La [tabla 4-30](#) proporciona información sobre los valores de la página **Configuración de la comunicación en serie en la LAN**.
- Haga clic en **Aplicar cambios**.
- Si es necesario, defina la configuración avanzada. De lo contrario, haga clic en el botón adecuado de la página **Configuración de la comunicación en serie en la LAN** para continuar (consulte la [tabla 4-31](#)).

Para definir la configuración avanzada, realice los pasos siguientes:

- Haga clic en **Configuración avanzada**.
- En la página **Configuración avanzada de la comunicación en serie en la LAN**, defina la configuración avanzada según sea necesario. Consulte la [tabla 4-32](#).
- Haga clic en **Aplicar cambios**.
- Para continuar, haga clic en el botón adecuado de la página **Configuración avanzada de la comunicación en serie en la LAN**. Consulte la [tabla 4-33](#).

Tabla 4-30. 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. Seleccionado = activada; deseleccionado = desactivada |
| Velocidad en baudios | La velocidad de los datos de IPMI. Seleccione 9600 bps , 19,2 kbps , 57,6 kbps o 115,2 kbps . |
| Límite de nivel de privilegio del canal | Establece el privilegio mínimo de usuario de la comunicación en serie en la LAN de IPMI: Administrador , Operador o Usuario . |

Tabla 4-31. 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 4-32. 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 comenzar a transmitir un paquete parcial de datos de caracteres de SOL. Incrementos de 5 ms a partir de 1. |
| Umbral de envío de caracteres | Tan pronto como se haya aceptado este número de caracteres (o más), el BMC enviará un paquete de datos de SOL con los caracteres. Unidades a partir de 1. |

Tabla 4-33. 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 . |

Configuración de servicios

 **NOTA:** Para modificar estos valores, usted debe tener permiso para **Configurar el DRAC 5**. Además, la utilidad de línea de comandos de RACADM remoto sólo se puede activar si el usuario ha iniciado sesión como usuario root.

1. Expanda el árbol de **Sistema**, 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:
 - 1 Servidor de web ([tabla 4-34](#))
 - 1 SSH ([tabla 4-35](#))
 - 1 Telnet ([tabla 4-36](#))
 - 1 RACADM remoto ([tabla 4-37](#))
 - 1 Agente de SNMP ([tabla 4-38](#))
 - 1 Agente de recuperación automatizada de sistemas ([tabla 4-39](#))

Use el **Agente de recuperación automatizada de sistemas** para activar la función **Pantalla de último bloqueo** del DRAC 5.

 **NOTA:** Para que la **Pantalla de último bloqueo** funcione en el DRAC 5, Server Administrator debe estar instalado con la función de **Recuperación automática** activada estableciendo **Acción** como: **Reiniciar sistema**, **Apagar el sistema**, o bien, **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 la [tabla 4-40](#).

Tabla 4-34. Configuración del servidor de web

| Valor | Descripción |
|-------------------------------|--|
| Activado | Activa o desactiva el servidor de web. Seleccionado = activado; deseleccionado = desactivado |
| Nº máx. de sesiones | El número máximo de sesiones simultáneas que se permiten para este sistema. |
| Sesiones activas | El número actual de sesiones en el sistema, menor o igual que el Nº máx. de sesiones . |
| Tiempo de espera | El tiempo en segundos que se permite que una conexión permanezca sin actividad. Cuando se alcanza el tiempo de espera, la sesión se cancela. Los cambios en el valor del tiempo de espera no afectan la sesión actual. Cuando se cambia el valor del tiempo de espera, se debe cerrar la sesión y volver a abrirla a fin de que el nuevo valor surta efecto. El rango del tiempo de espera es de 60 a 1920 segundos. |
| Número de puerto HTTP | El puerto que el DRAC usa para detectar una conexión de servidor. El valor predeterminado es 80 . |
| Número de puerto HTTPS | El puerto en que el DRAC busca una conexión de servidor. El valor predeterminado es 443 . |

Tabla 4-35. Configuración de SSH

| Valor | Descripción |
|----------------------------|--|
| Activado | Activa o desactiva SSH. Seleccionado = activado; deseleccionado = desactivado |
| Nº máx. de sesiones | El número máximo de sesiones simultáneas que se permiten para este sistema. Se admiten hasta cuatro sesiones. |
| Sesiones activas | El número actual de sesiones en el sistema, menor o igual que el Nº máx. de sesiones . |
| Tiempo de espera | El tiempo de espera sin actividad de Secure Shell, en segundos. Rango = de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es 300 . |
| Número de puerto | El puerto en que el DRAC busca una conexión de servidor. El valor predeterminado es 22 . |

Tabla 4-36. Configuración de Telnet

| Valor | Descripción |
|----------------------------|--|
| Activado | Activa o desactiva Telnet. Seleccionado = activado; deseleccionado = desactivado |
| Nº máx. de sesiones | El número máximo de sesiones simultáneas que se permiten para este sistema. Se admiten hasta cuatro sesiones. |
| Sesiones activas | El número actual de sesiones en el sistema, menor o igual que el Nº máx. de sesiones . |
| Tiempo de espera | El tiempo de espera sin actividad de Secure Shell, en segundos. Rango = de 60 a 1920 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es 0 . |
| Número de puerto | El puerto en que el DRAC busca una conexión de servidor. El valor predeterminado es 23 . |

Tabla 4-37. Configuración de RACADM remoto

| Valor | Descripción |
|----------------------------|---|
| Activado | Activa o desactiva RACADM remoto. Seleccionado = activado; deseleccionado = desactivado |
| Nº máx. de sesiones | El número máximo de sesiones simultáneas que se permiten para este sistema. Se admiten hasta cuatro sesiones. |
| Sesiones activas | El número actual de sesiones en el sistema, menor o igual que el Nº máx. de sesiones . |

Tabla 4-38. Configuración del agente de SNMP

| Valor | Descripción |
|----------------------------|---|
| Activado | Activa o desactiva el agente de SNMP. Seleccionado = activado; deseleccionado = 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 y sin espacios en blanco. El valor predeterminado es public . |

Tabla 4-39. Valor del agente de recuperación automatizada de sistemas

| Valor | Descripción |
|-------|-------------|
| | |

| | |
|-----------------|--|
| Activado | Activa el agente de recuperación automatizada de sistemas. |
|-----------------|--|

Tabla 4-40. Botones de la página de servicios

| Botón | Descripción |
|-----------------|--|
| Imprimir | Imprime la página Servicios. |
| Actualizar | Actualiza la página Servicios. |
| Aplicar cambios | Aplica los valores de la página Servicios. |

Preguntas frecuentes

La [tabla 4-41](#) muestra una lista de preguntas y respuestas frecuentes.

Tabla 4-41. Administración y recuperación de un sistema remoto: Preguntas frecuentes

| Pregunta | Respuesta |
|--|--|
| Al acceder a la interfaz por web del DRAC 5, recibo una advertencia de seguridad informando que el nombre del host del certificado SSL no coincide con el nombre de host del DRAC 5. | <p>El DRAC 5 incluye un certificado de servidor predeterminado del DRAC 5 para garantizar la seguridad de red de las funciones de la interfaz por web y el racadm remoto. Cuando se usa este certificado, el explorador de web muestra una advertencia de seguridad porque el certificado predeterminado fue emitido para el Certificado predeterminado del DRAC5 y éste no coincide con el nombre de host del DRAC 5 (por ejemplo, en cuanto a la dirección IP).</p> <p>Para resolver este asunto de seguridad, cargue un certificado de servidor del DRAC 5 que haya sido creado para la dirección IP del DRAC 5. Al generar la solicitud de firma de certificado (CSR) que se usará para emitir el certificado, asegúrese que el nombre común (CN) del CSR tenga la misma dirección IP del DRAC 5 (por ejemplo, 192.168.0.120) o el nombre DNS registrado del DRAC.</p> <p>Para asegurarse que la CSR coincida con el nombre DNS registrado del DRAC, realice los pasos a continuación:</p> <ol style="list-style-type: none"> 1. En el árbol de Sistema, haga clic en Acceso remoto. 2. Haga clic en la ficha Configuración y después haga clic en Red. 3. En la página Configuración de la red, realice los pasos a continuación: <ol style="list-style-type: none"> a. Seleccione la casilla Registrar el DRAC en DNS. b. En el campo Nombre DNS del DRAC, introduzca el nombre del DRAC. 4. Haga clic en Aplicar cambios. <p>Consulte "Cómo asegurar las comunicaciones del DRAC 5 por medio de certificados SSL y digitales" para obtener más información acerca de cómo generar las CSR y cómo emitir certificados.</p> |
| ¿Por qué no están disponibles los servicios racadm remoto y servicios a base de Web después de un cambio de propiedad? | <p>Es posible que los servicios racadm remotos y la interfaz basada en web tarden un minuto en estar disponibles después de que se restablezca el Web Server del DRAC 5.</p> <p>El Web server DRAC 5 se restablece después de los acontecimientos siguientes:</p> <ol style="list-style-type: none"> 1 Cuando se cambia la configuración de la red o las propiedades de seguridad de la red por medio de la interfaz de web de usuario del DRAC 5 1 Cuando se cambia la propiedad <code>cfgRacTuneHttpsPort</code> (incluso cuando un comando <code>config -f <archivo de config></code> lo cambia) 1 Cuando se usa <code>racresetcfg</code> 1 Cuando se restablece el DRAC 5 1 Cuando se carga un nuevo certificado de servidor SSL |
| ¿Por qué no registra mi servidor DNS mi DRAC 5? | Algunos servidores DNS sólo registran nombres de 31 caracteres o menos. |
| Al acceder a la interfaz por web del DRAC 5, recibo una advertencia de seguridad informando 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 del DRAC 5 para garantizar la seguridad de red de las funciones de la interfaz por web y de racadm remoto. Este certificado no fue emitido por CA confiable. Para resolver este asunto de seguridad , cargue un certificado de servidor de DRAC 5 que haya sido publicado por una CA confiable (por ejemplo, Thawte o Verisign). Consulte " Cómo asegurar las comunicaciones del DRAC 5 por medio de certificados SSL y digitales " para obtener más información acerca de cómo emitir certificados. |
| <p>El mensaje siguiente se muestra por motivos desconocidos:</p> <p>Remote Access: SNMP Authentication Failure</p> <p>(Acceso remoto: falla de autenticación de SNMP)</p> <p>¿Por qué sucede esto?</p> | <p>Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad "get" y "set" del dispositivo. En IT Assistant, se tiene el nombre <code>get nombre de comunidad = public</code> (público) y el nombre <code>set nombre de comunidad = private</code> (privado). De manera predeterminada, el nombre de comunidad para el agente DRAC 5 es "public" (público). Cuando IT Assistant envía una solicitud "set", el agente DRAC 5 genera un error de autenticación SNMP debido a que sólo acepta peticiones de <code>comunidad = public</code> (público).</p> <p>Puede cambiar el nombre de comunidad del DRAC 5 usando el comando RACADM.</p> <p>Para ver el nombre de comunidad del DRAC 5, use el comando siguiente:</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>Para establecer el nombre de comunidad del DRAC 5, use el comando siguiente:</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nombre de comunidad></pre> <p>Para evitar que se generen capturas de autenticación SNMP, debe de introducir nombres de comunidad que acepte el agente. Como el DRAC 5 sólo permite un nombre de comunidad, debe introducir el mismo nombre de comunidad para los comandos <code>get</code> y <code>set</code> para la configuración de descubrimiento de IT Assistant.</p> |

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Recuperación y solución de problemas del sistema administrado

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Primero pasos para solucionar problemas de un sistema remoto](#)
- [Administración de alimentación en un sistema remoto](#)
- [Visualización de información del sistema](#)
- [Uso del registro de sucesos del sistema \(SEL\)](#)
- [Visualización de la pantalla de último bloqueo del sistema](#)
- [Uso del registro del RAC](#)
- [Uso de la consola de diagnósticos](#)
- [Solución de problemas de red](#)
- [Solución de problemas de alertas](#)

Esta sección explica cómo realizar tareas relacionadas con la recuperación y solución de problemas de un sistema remoto bloqueado con la interfaz basada en web del DRAC 5. Para obtener información de solución de problemas del DRAC 5, consulte "[Instalación del sistema operativo por medio de VM-CLI](#)".

- 1 Solución de problemas de un sistema remoto
- 1 Administración de alimentación en un sistema remoto
- 1 Uso del registro de sucesos del sistema (SEL)
- 1 Visualización de la pantalla de último bloqueo del sistema
- 1 Uso del registro del RAC
- 1 Uso de la consola de diagnósticos

Primero pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas de alto nivel en el sistema administrado:

1. ¿El sistema está encendido o apagado?
2. Si 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 "[Visualización de la pantalla de último bloqueo del sistema](#)") y utilice la redirección de consola ("[Frecuencias de actualización de las resoluciones de pantalla admitidas en el sistema administrado](#)") y la administración de alimentación remota (consulte "[Administración de alimentación en un sistema remoto](#)") para reiniciar el sistema y vigilar el proceso de reinicio.

Administración de alimentación en un sistema remoto

El DRAC 5 le permite realizar de forma remota varias acciones de administración de alimentación en el sistema administrado para que pueda recuperarse después de un bloqueo del sistema o de otros sucesos del sistema.

Use la página **Administración de la alimentación** para hacer lo siguiente:

- 1 Realice un apagado ordenado por medio del sistema operativo cuando reinicie, y encienda o apague el sistema.
- 1 Consulte el **Estado de la alimentación** actual del sistema: **Encendido** o **Apagado**.

Para acceder a la página **Administración de la alimentación** del árbol de Sistema, haga clic en **Sistema** y luego 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 acciones de control de alimentación

1. Seleccione una de las siguientes **Acciones de control de alimentación**.
 - 1 **Encender el sistema:** enciende el sistema (equivalente a pulsar el botón de encendido cuando el sistema está apagado).
 - 1 **Apagar el sistema:** apaga el sistema (equivalente a pulsar el botón de encendido cuando el sistema está encendido).
 - 1 **Restablecer el sistema:** restablece el sistema (equivalente a pulsar el botón de restablecimiento); el sistema no se apaga con el uso de esta función.
 - 1 **Realizar ciclo de encendido del sistema:** apaga el sistema y luego lo reinicia (reinicio mediante suministro de energía).
2. Haga clic en **Aplicar** para realizar la acción de administración de alimentación (por ejemplo, haga que el sistema realice un ciclo de encendido).
3. Para continuar, haga clic en el botón adecuado de la página **Administración de la alimentación** (consulte la [tabla 5-1](#)).

Tabla 5-1. Botones de la página de administración de la alimentación (esquina superior derecha)

| Botón | Acción |
|------------|--|
| Imprimir | Imprime la página Administración de la alimentación |
| Actualizar | Vuelve a cargar la página Administración de la alimentación |

Visualización de información del sistema

La página Resumen del sistema muestra información acerca de los siguientes componentes del sistema:

- 1 Chasis del sistema principal
- 1 Remote Access Controller
- 1 Controlador de administración de la placa base

Para acceder a la información del sistema, expanda el árbol de **Sistema** y haga clic en **Propiedades**.

Chasis del sistema principal

La [tabla 5-2](#) y la [tabla 5-3](#) describen las propiedades del chasis del sistema principal.

 **NOTA:** Para recibir información sobre el **Nombre del host** y **Nombre del sistema operativo**, debe tener los servicios del DRAC 5 instalados en el sistema administrado.

Tabla 5-2. Campos de información del sistema

| Campo | Descripción |
|-----------------------------|--|
| Descripción | Descripción del sistema. |
| Versión del BIOS | Versión del BIOS del sistema. |
| Etiqueta de servicio | Número de etiqueta de servicio del sistema. |
| Nombre del host | Nombre del sistema host. |
| Nombre del OS | El sistema operativo que se está ejecutando en el sistema. |

Tabla 5-3. Campos de la recuperación automática

| Campo | Descripción |
|---------------------------------|--|
| Acción de recuperación | Cuando un se detecta un "bloqueo del sistema", el DRAC puede configurarse para que lleve a cabo una de las acciones siguientes: ninguna acción, restablecimiento forzado, apagar o ciclo de encendido. |
| Cuenta regresiva inicial | El número de segundos después de detectar un "bloqueo del sistema" al término de los cuales el DRAC realizará una acción de recuperación. |
| Cuenta regresiva actual | El valor actual, en segundos, del temporizador de cuenta regresiva. |

Remote Access Controller

La [tabla 5-4](#) describe las propiedades del Remote Access Controller.

Tabla 5-4. Campos de información del RAC

| Campo | Descripción |
|---------------------------------|---|
| Nombre | Nombre corto. |
| Información del producto | Nombre detallado. |
| Versión del hardware | La versión de la tarjeta Remote Access Controller, o bien, "desconocida". |
| Versión del firmware | El nivel de versión del firmware actual del DRAC 5. |
| Firmware actualizado | Fecha y hora en la que el firmware se actualizó por última vez. |
| Hora del RAC | Hora del reloj del sistema. |

Controlador de administración de la placa base

La [tabla 5-5](#) describe las propiedades del controlador de administración de la placa base.

Tabla 5-5. Campos de información del BMC

| Campo | Descripción |
|------------------------------------|---|
| Nombre | "Controlador de administración de la placa base". |
| Versión de IPMI | La versión de la Interfaz de administración de plataforma inteligente (IPMI). |
| Número posible de sesiones activas | El número máximo de sesiones que pueden estar activas al mismo tiempo. |
| Número actual de sesiones activas | El número total de sesiones actualmente activas. |
| Versión del firmware | La versión del firmware del BMC. |
| LAN activada | LAN activada o LAN desactivada. |

Uso del registro de sucesos del sistema (SEL)

La página **Registro SEL** muestra los sucesos críticos de sistema que ocurren en el sistema administrado.

Para ver el registro de sucesos del sistema, realice los pasos a continuación:

1. En el árbol de **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 de los sucesos y proporciona otra información según se muestra en la [tabla 5-6](#).

3. Para continuar, haga clic en el botón adecuado de la página **Registro de sucesos del sistema** (consulte la [tabla 5-7](#)).

Tabla 5-6. 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 de signo de interrogación indica que el estado es desconocido. |
| Fecha/hora | La fecha y hora en que ocurrió el suceso. Si la fecha está en blanco, el suceso ocurrió durante el inicio del sistema. El formato es mm/dd/aaaa hh:mm:ss, expresado en formato de 24 horas. |
| Descripción | Breve descripción del suceso |

Tabla 5-7. Botones de la página de SEL

| Botón | Acción |
|-----------------|--|
| Imprimir | Imprime el SEL en el orden que aparece en la ventana. |
| Borrar registro | Borra el SEL. NOTA: El botón Borrar registro sólo aparece si tiene permiso de Borrar registros . |
| Guardar como | Abre una ventana emergente que le permite guardar el SEL en un directorio de su elección. |
| Actualizar | Recarga la página SEL. |

Visualización de la pantalla de último bloqueo del sistema

-  **AVISO:** La función de pantalla de último bloqueo requiere que el sistema tenga la función **Recuperación Automática** configurada en Server Administrator. Además, asegúrese que la función **Recuperación automatizada de sistema** está activada por medio del DRAC. Desplácese hasta 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 de bloqueo más reciente, que incluye información sobre los sucesos que ocurrieron antes de que el sistema se bloquee. La información del último bloqueo del sistema se guarda en la memoria del DRAC 5 y se puede acceder a la misma de forma remota.

Para ver la página **Pantalla de último bloqueo**, realice los pasos a continuación:

1. En el árbol de **Sistema**, haga clic en **Sistema**.
2. Haga clic en la ficha **Registros** y luego haga clic en **Último bloqueo**.

La página **Pantalla de último bloqueo** proporciona los botones siguientes (consulte la [tabla 5-8](#)) en la esquina superior derecha de la pantalla:

Tabla 5-8. Botones de página de pantalla de último bloqueo

| Botón | Acción |
|------------|--|
| Imprimir | Imprime la página Pantalla de último bloqueo . |
| Guardar | Abre una ventana emergente que le permite guardar la Pantalla de último bloqueo en un directorio de su elección. |
| Eliminar | Elimina la página Pantalla de último bloqueo . |
| Actualizar | Recarga la página Pantalla de último bloqueo . |

 **NOTA:** Debido a fluctuaciones en el temporizador de la recuperación automático, es posible que la **Pantalla de último bloqueo** no pueda ser capturada cuando el temporizador de restablecimiento del sistema esté definido con un valor menor de 30 segundos. Utilice Server Administrator o IT Assistant para definir el temporizador de restablecimiento del sistema como al menos 30 segundos y para asegurarse de que la **Pantalla de último bloqueo** funcione correctamente. Para obtener información adicional, consulte "[Configuración del sistema administrado para capturar la pantalla de último bloqueo](#)".

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 (como inicio y cierre de sesión, y cambios de las políticas 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, realice los pasos siguientes:

1. En el árbol de **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 de la [tabla 5-9](#).

Tabla 5-9. Información de la página de registro del RAC

| Icono | Descripción |
|-------------|--|
| Fecha/hora | La fecha y hora (por ejemplo, 19 de dic., 16:55:47). Cuando el DRAC 5 arranca inicialmente y no puede comunicarse con el sistema administrado, el tiempo mostrado representará el tiempo que ha transcurrido desde que se inició el DRAC 5. El DRAC 5 supondrá que inició el jueves 1º de enero de 1970 a las 00:00:00. |
| Origen | La interfaz que ocasionó el suceso. |
| Descripción | Una breve descripción del suceso y el nombre de usuario que inició sesión en el DRAC 5. |

Uso de los botones de página de registro del DRAC 5

La página **Registro del RAC** tiene los siguientes botones (consulte la [tabla 5-10](#)).

Tabla 5-10. Botones de registro del DRAC 5

| Botón | Acción |
|-----------------|---|
| Imprimir | Imprime la página Registro del DRAC 5 . |
| Borrar registro | Borra las anotaciones del Registro del DRAC 5 . NOTA: El botón Borrar registro sólo aparece si tiene permiso de Borrar registros . |
| Guardar como | Abre una ventana emergente que le permite guardar el Registro del DRAC 5 en un directorio de su elección. |
| Actualizar | Vuelve a cargar la página del Registro del DRAC 5 . |

Uso de la consola de diagnósticos

El DRAC 5 proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la [tabla 5-11](#)) que es parecido a las herramientas que incluyen los sistemas 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 tener acceso a la página **Consola de diagnósticos**, realice los pasos a continuación:

1. En el árbol de **Sistema**, haga clic en **Acceso remoto**.
2. Haga clic en la ficha **Diagnósticos**.

La [tabla 5-11](#) describe las opciones que están disponibles en la página **Consola de diagnósticos**. Escriba un comando y haga clic en **Enviar**. Los resultados de depuración aparecerán en la página **Consola de diagnósticos**.

Para actualizar la página **Consola de diagnósticos**, haga clic en **Actualizar**. Para ejecutar otro comando, haga clic en **Volver a la página de diagnósticos**.

Tabla 5-11. Comandos de diagnóstico

| Comando | Descripción |
|------------------------|--|
| arp | Muestra el contenido de la tabla del Protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar. |
| ifconfig | Muestra el contenido de la tabla de interfaz de red. |
| netstat | Imprime el contenido de la tabla de enrutamiento. Si se proporciona el número de interfaz opcional en el campo de texto situado a la derecha de la opción netstat , dicha opción imprime información adicional acerca del tráfico 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 introducir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control en Internet) se envía a la dirección IP de destino basada en el contenido de tabla de enrutamiento actual. |
| gettracelog | Muestra del registro de rastreo del DRAC 5. Para obtener más información, consulte " gettracelog ". |

Solución de problemas de red

Los administradores usan el registro de rastreo interno del DRAC 5 para depurar las alertas o el sistema de red de este último. Puede acceder al registro de rastreo a partir de la interfaz basada en web del DRAC 5 si hace clic en la ficha **Diagnósticos** y luego escribe el comando **gettracelog** o el comando **racadm gettracelog**. Para obtener más información, consulte "[gettracelog](#)".

El registro de rastreo vigila la siguiente información:

- 1 DHCP: rastrea paquetes enviados y recibidos desde un servidor DHCP.
- 1 IP: rastrea paquetes IP enviados y recibidos.

El registro de rastreo puede contener también códigos de error específicos del firmware del DRAC 5 que están relacionados con el firmware del DRAC 5 interno, no con el sistema operativo del sistema administrado.

 **NOTA:** El DRAC 5 no generará un eco por un ICMP (ping) con un tamaño de paquete más grande que 1500 bytes.

Solución de problemas de alertas

Utilice la información de captura SNMP registrada para solucionar problemas de un tipo particular de alerta del DRAC 5. Las entregas de captura SNMP se registran en el Registro de rastreo de forma predeterminada. Sin embargo, ya que SNMP no confirma la entrega de capturas, utilice un analizador de red o una herramienta como **snmputil** de Microsoft para rastrear los paquetes en el sistema administrado.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso del DRAC 5 con Microsoft Active Directory

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Ampliaciones de esquema de Active Directory](#)
- [Descripción de las ampliaciones de esquema del RAC](#)
- [Descripción de objetos de Active Directory](#)
- [Configuración de Active Directory para acceder al DRAC 5](#)
- [Ampliación del esquema de Active Directory](#)
- [Instalación de la extensión de Dell para el complemento de equipos y usuarios de Active Directory](#)
- [Cómo agregar usuarios y privilegios del DRAC 5 a Active Directory](#)
- [Habilitación de SSL en un controlador de dominio](#)
- [Configuración del DRAC 5](#)
- [Uso de Active Directory para iniciar sesión en el DRAC 5](#)
- [Preguntas frecuentes](#)

Un servicio de directorio mantiene una base de datos común de toda la información necesaria para controlar usuarios, equipos, impresoras, etc., en una red. Si su empresa usa el software de servicio Microsoft® Active Directory®, usted puede configurarlo de manera que tenga acceso al DRAC 5, lo que le permite agregar y controlar los privilegios de usuario del DRAC 5 de los usuarios existentes en el software Active Directory.

 **NOTA:** El uso de Active Directory para reconocer a los usuarios del DRAC 5 se admite en los sistemas operativos Microsoft Windows 2000 y Windows Server 2003.

Ampliaciones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario pueden incluir el nombre, apellido, número de teléfono del usuario, etcétera. Las empresas pueden ampliar la base de datos de Active Directory agregando sus propios atributos y clases únicas para atender a las necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autenticación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory se debe definir con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de identificadores de objeto (OID) de Active Directory de modo que cuando las empresas agregan extensiones al esquema, pueden tener la garantía de que son únicas y que no tendrán conflictos entre sí. Para ampliar el esquema en Active Directory de Microsoft, Dell recibió OID únicas, extensiones de nombre únicas e identificaciones de atributos vinculados de manera única para nuestros atributos y clases que se agregaron al servicio de directorio.

La extensión Dell es: dell

El OID base 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 Microsoft mantiene se puede consultar en <http://msdn.microsoft.com/certification/ADAcctInfo.asp> al introducir la extensión de Dell.

Descripción de las ampliaciones de esquema del RAC

Para proporcionar la mayor flexibilidad en la multitud de entornos de los clientes, Dell proporciona un grupo de propiedades que el usuario puede configurar en función de los resultados deseados. Dell ha ampliado el esquema para incluir las propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos de RAC. Este modelo ofrece la máxima flexibilidad a un administrador para las distintas combinaciones de usuarios, privilegios y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción de objetos de Active Directory

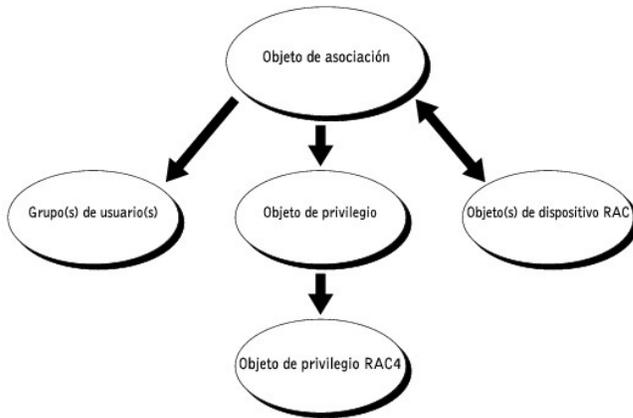
Para cada uno de los RAC físicos en la red que desee integrar con Active Directory para la autenticación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo de RAC. Puede crear varios objetos de asociación y cada uno de ellos se puede vincular a los usuarios, grupos de usuarios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

Sin embargo, cada objeto de asociación puede estar vinculado sólo a un objeto de privilegio (o bien, puede vincular usuarios, grupos de usuarios u objetos de dispositivo de RAC). Este ejemplo permite que un administrador controle los privilegios de cada usuario en RAC específicos.

El objeto del dispositivo del RAC es el eslabón al firmware de RAC para consultar a Active Directory para la autenticación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y el objeto de dispositivo con el nombre de Active Directory de manera que los usuarios puedan llevar a cabo la autenticación y autorización con Active Directory. Además, el administrador también deberá agregar el RAC por lo menos a un objeto de asociación para que los usuarios se puedan autenticar.

La [figura 6-1](#) ilustra que el objeto de asociación proporciona la conexión que es necesaria para toda la autenticación y autorización.

Figura 6-1. Configuración típica de los objetos de Active Directory



NOTA: El objeto de privilegio del RAC se aplica al DRAC 4 y al DRAC 5.

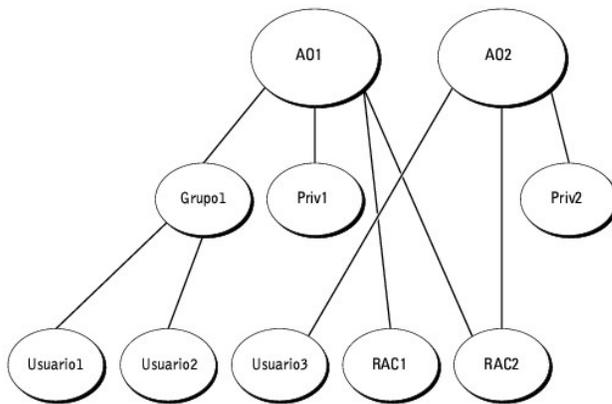
Usted puede crear la cantidad de objetos de asociación que necesite. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de RAC para cada RAC (DRAC 5) en la red que desea integrar con Active Directory para fines de autenticación y autorización con el RAC (DRAC 5).

El objeto de asociación tiene capacidad para cualquier cantidad de usuarios y/o grupos, así como de objetos de dispositivo de RAC. Sin embargo, el objeto de asociación incluye únicamente un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los "Usuarios" que tienen "Privilegios" en los RAC (DRAC 5s).

Además, puede configurar objetos de Active Directory en un solo dominio o en múltiples dominios. Por ejemplo, digamos que usted tiene dos tarjetas DRAC 5 (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). Usted desea dar privilegios de administrador a usuario1 y usuario2 para las dos tarjetas DRAC 5 y quiere dar privilegio de inicio de sesión a usuario3 para la tarjeta RAC2. La [figura 6-2](#) le muestra cómo configurar los objetos de Active Directory en este escenario.

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

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



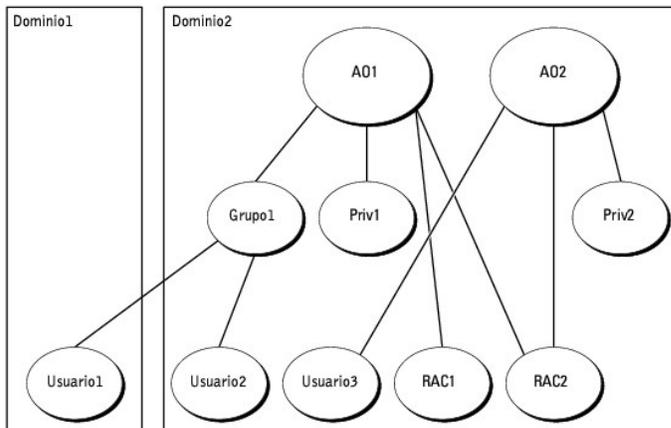
Para configurar los objetos para el escenario de un solo dominio, realice las siguientes tareas:

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC -RAC1 y RAC2- para representar las dos tarjetas DRAC 5.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde el Priv1 tiene todos los privilegios (administrador) y Priv2 tiene privilegios de inicio de sesión.
4. Agrupe usuario1 y usuario2 en el Grupo1.
5. Agregue a Grupo1 como miembro en el objeto de asociación 1 (A01), Priv1 como objeto de privilegio en A01, y RAC1, RAC2 como dispositivos RAC en A01.
6. Agregue al usuario3 como miembro en el objeto de asociación 2 (A02), Priv2 como objeto de privilegio en A02, y RAC2 como dispositivos de RAC en A02.

Consulte "[Cómo agregar usuarios y privilegios del DRAC 5 a Active Directory](#)" para ver instrucciones detalladas.

La [figura 6-3](#) muestra un ejemplo de objetos de Active Directory en varios dominios. En este escenario, usted tiene dos tarjetas DRAC 5 (RAC1 y RAC2) y tres usuarios existentes de Active Directory (usuario1, usuario2 y usuario3). El usuario1 está en el dominio1, y el usuario2 y el usuario3 están en el dominio2. En este escenario, configure el usuario1 y el usuario2 con privilegios de administrador en las dos tarjetas DRAC 5 y configure el usuario3 con privilegios de inicio de sesión para la tarjeta RAC2.

Figura 6-3. Configuración de los objetos de Active Directory en varios dominios



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

1. Asegúrese que la función de bosque de dominio esté en los modos Nativo o Windows 2003.
2. Cree dos objetos de asociación, AO1 (de alcance universal) y AO2, en cualquier dominio.
La [figura 6-3](#) muestra los objetos en el Dominio2.
3. Cree dos objetos de dispositivo de RAC -RAC1 y RAC2- para representar 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 usuario1 y usuario2 en el Grupo1. El alcance de grupo de Grupo1 debe ser universal.
6. Agregue al Grupo1 como miembros en el objeto de asociación 1 (AO1), Priv1 como objeto de privilegio en AO1, y RAC1, RAC2 como dispositivos RAC en AO1.
7. Agregue al usuario3 como miembro en el objeto de asociación 2 (AO2), Priv2 como objeto de privilegio en AO2, y RAC2 como dispositivos de RAC en AO2.

Configuración de Active Directory para acceder al DRAC 5

Antes de usar el Active Directory para acceder al DRAC 5, debe configurar el software Active Directory y el DRAC 5 llevando a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema Active Directory (consulte "[Ampliación del esquema de Active Directory](#)").
2. Extienda el complemento de equipos y usuarios de Active Directory (consulte "[Instalación de la extensión de Dell para el complemento de equipos y usuarios de Active Directory](#)").
3. Agregue los usuarios del DRAC 5 y sus privilegios al Active Directory (consulte "[Cómo agregar usuarios y privilegios del DRAC 5 a Active Directory](#)").
4. Habilite SSL en cada uno de los controladores de dominio (consulte "[Habilitación de SSL en un controlador de dominio](#)").
5. Configure las propiedades de Active Directory del DRAC 5 por medio de la interfaz basada en web del DRAC 5 o de RACADM (consulte "[Configuración del DRAC 5](#)").

Ampliación del esquema de Active Directory

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

Puede ampliar su esquema usando uno de los métodos siguientes:

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

Si usa el archivo de secuencia de comandos LDIF, la unidad organizativa Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el CD *Dell Systems Management Consoles* en los siguientes directorios respectivamente:

- 1 *Unidad de CD:\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files*
- 1 *Unidad de CD:\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender*

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, realice los pasos en "[Utilización de ampliador de esquema de Dell](#)".

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

Uso de Dell Schema Extender

 **AVISO:** Dell Schema Extender usa el archivo **SchemaExtenderOem.ini**. Para asegurar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla **Bienvenido**, haga clic en **Siguiente**.
2. Lea detenidamente la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales actuales de inicio de sesión** o introduzca un nombre de usuario y contraseña con derechos de administrador de esquema .
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Terminar**.

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

- 1 Clases (consulte de la [tabla 6-1](#) a la [tabla 6-6](#))
- 1 Atributos ([tabla 6-7](#))

Consulte la documentación de Microsoft para obtener más información acerca de cómo habilitar y usar el complemento de esquema de Active Directory en el MMC.

Tabla 6-1. Definiciones de las clases agregadas al esquema de Active Directory

| Nombre de clase | Número de identificación del objeto asignado (OID) |
|-----------------------|--|
| dellRacDevice | 1.2.840.113556.1.8000.1280.1.1.1.1 |
| dellAssociationObject | 1.2.840.113556.1.8000.1280.1.1.1.2 |
| dellRACPrivileges | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| dellPrivileges | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| dellProduct | 1.2.840.113556.1.8000.1280.1.1.1.5 |

Tabla 6-2. Clase dellRacDevice

| | |
|---------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.1 |
| Descripción | Representa el dispositivo de RAC de Dell. El dispositivo de RAC debe ser configurado como dellRacDevice en Active Directory. Esta configuración hace posible que el DRAC 5 envíe consultas de Protocolo de acceso ligero de directorio (LDAP) al Active Directory. |
| Tipo de clase | Clase estructural |
| Súper clases | dellProduct |
| Atributos | dellSchemaVersion dellRacType |

Tabla 6-3. Clase dellAssociationObject

| | |
|--|--|
| | |
|--|--|

| | |
|---------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.2 |
| Descripción | Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos. |
| Tipo de clase | Clase estructural |
| Súper clases | Grupo |
| Atributos | dellProductMembers dellPrivilegeMember |

Tabla 6-4. Clase dellRac4Privileges

| | |
|---------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| Descripción | Se usa para definir los privilegios (derechos de autorización) del dispositivo DRAC 5. |
| Tipo de clase | Clase auxiliar |
| Súper clases | Ninguna |
| Atributos | dell sLoginUser dell sCardConfigAdmin dell sUserConfigAdmin dell sLogClearAdmin dell sServerResetUser dell sConsoleRedirectUser dell sVirtualMediaUser dell sTestAlertUser dell sDebugCommandAdmin |

Tabla 6-5. Clase dellPrivileges

| | |
|---------------|--|
| OID | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| Descripción | Se usa como clase de contenedor para los privilegios (derechos de autorización) de Dell. |
| Tipo de clase | Clase estructural |
| Súper clases | Usuario |
| Atributos | dellRAC4Privileges |

Tabla 6-6. Clase dellProduct

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

Tabla 6-7. Lista de atributos agregados al esquema de Active Directory

| Nombre/descripción del atributo | OID asignada/sintaxis del identificador de objeto | Valor único |
|---|--|-------------|
| dellPrivilegeMember Lista los objetos de dellPrivilege que pertenecen a este atributo. | 1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| dellProductMembers Lista los objetos de dellRacDevices que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso de dellAssociationMembers. Identificación de vínculo: 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| dell sLoginUser Es "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 |

| | | |
|---|---|-------|
| dell sCardConfigAdmin Es "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 |
| dell sUserConfigAdmin Es "TRUE" si el usuario tiene derechos de configuración de usuarios en el dispositivo. | 1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dell sLogClearAdmin Es "TRUE" si el usuario tiene derechos para borrar el registro en el dispositivo. | 1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dell sServerResetUser Es "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 |
| dell sConsoleRedirectUser Es "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 |
| dell sVirtualMediaUser Es "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 |
| dell sTestAlertUser Es "TRUE" si el usuario tiene derechos de prueba de alertas de usuario en el dispositivo. | 1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dell sDebugCommandAdmin Es "TRUE" si el usuario tiene derechos de administrador del comando de depuración en el dispositivo. | 1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| dell SchemaVersion Se usa la versión del esquema actual para actualizar el esquema. | 1.2.840.113556.1.8000.1280.1.1.2.12 Cadena para ignorar mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| dell RacType Este atributo es el tipo de RAC actual del objeto dellRacDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers. | 1.2.840.113556.1.8000.1280.1.1.2.13 Cadena para ignorar mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| dell AssociationMembers Lista los miembros dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo ligado de dellProductMembers. Identificación de vínculo: 12071 | 1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |

Instalación de la extensión Dell en el complemento de usuarios y equipos de Active Directory

Cuando usted amplía el esquema en Active Directory, debe ampliar también el complemento de usuarios y equipos de Active Directory de manera que el administrador pueda controlar los dispositivos de RAC (DRAC 5), los usuarios y los grupos de usuarios, las asociaciones de RAC y los privilegios de RAC.

Cuando instala el software de administración de sistemas con el CD *Dell Systems Management Consoles*, puede extender el complemento seleccionando 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 ver instrucciones adicionales de instalación del software Systems Management.

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

Instalación del paquete de administrador

Debe instalar el paquete de administrador en cada sistema que administre los objetos de DRAC 5 de Active Directory. Si no instala el paquete de administrador, no podrá ver el objeto de RAC de Dell en el contenedor.

Para obtener más información, consulte "[Cómo abrir el complemento de usuarios y equipos de Active Directory](#)".

Apertura del complemento para equipos y usuarios de Active Directory

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

1. Si tiene una sesión abierta en el controlador de dominio, haga clic en **Inicio Herramientas administrativas** → **Usuarios y computadoras de Active Directory**.

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

Aparecerá el servicio Microsoft Management Console (MMC).

2. En la ventana **Consola 1**, haga clic en **Archivo** (o **Consola** en los sistemas que ejecutan Windows 2000).
3. Haga clic en **Agregar o quitar complemento**.
4. Seleccione el complemento **Usuarios y equipos de Active Directory** y haga clic en **Agregar**.
5. Haga clic en **Cerrar** y haga clic en **Aceptar**.

Cómo agregar usuarios y privilegios del DRAC 5 a Active Directory

Con el complemento de usuarios y equipos de Active Directory extendido de Dell, usted puede agregar usuarios y privilegios del DRAC 5 mediante la creación de objetos de RAC, de asociación y de privilegio. Para agregar cada tipo de objeto, realice los procedimientos siguientes:

- 1 Cree un objeto de dispositivo de RAC
- 1 Cree un objeto de privilegio
- 1 Cree un objeto de asociación
- 1 Agregue los objetos a un objeto de asociación

Creación de un objeto de dispositivo de RAC

1. En la ventana **Raíz de consola** en MMC, haga clic con el botón derecho del mouse sobre un contenedor.
2. Seleccione **Nuevo** → **Objeto de RAC de Dell**.
Aparecerá la ventana **Nuevo objeto**.
3. Teclee un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del DRAC 5 que teleará en el [paso 7](#) de "[Configuración del DRAC 5](#)".
4. Seleccione **Objeto de dispositivo de RAC**.
5. Haga clic en **Aceptar**.

Creación de un objeto de privilegio

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

1. En la ventana **Raíz de la consola** (en MMC), haga clic con el botón derecho del mouse sobre un contenedor.
2. Seleccione **Nuevo** → **objeto de RAC de Dell**.
Aparecerá la ventana **Nuevo objeto**.
3. Teclee un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **Aceptar**.
6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
7. Haga clic en la ficha **Privilegios de RAC** y seleccione los privilegios que desea que el usuario tenga (para obtener más información, consulte la [tabla 4-8](#)).

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El alcance de asociación especifica el tipo de grupo de seguridad del objeto

de asociación. Cuando cree un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objeto que quiere agregar.

Por ejemplo, si se selecciona **Universal**, los objetos de asociación estarán disponibles únicamente cuando el dominio de Active Directory esté funcionando en modo nativo o superior.

1. En la ventana **Raíz de la consola** (en MMC), haga clic con el botón derecho del mouse sobre un contenedor.
2. Seleccione **Nuevo**→ **objeto de RAC de Dell**.
Esto abrirá la ventana **Nuevo objeto**.
3. Teclee un nombre para el nuevo objeto.
4. Seleccione **Objeto de asociación**.
5. Seleccione el alcance para el **Objeto de asociación**.
6. Haga clic en **Aceptar**.

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades del objeto de asociación**, puede asociar a usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si su sistema ejecuta el modo Windows 2000 u otro superior, se deben usar grupos universales para extender los dominios con usuarios u objetos de RAC.

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

Cómo agregar usuarios o grupos de usuarios

1. Haga clic con el botón derecho del mouse en **Objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de usuario o del grupo de usuario y haga clic en **Aceptar**.

Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios de usuario o de grupo de usuarios al autenticar un dispositivo de RAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

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

Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados a la red que están disponibles para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de RAC a un objeto de asociación.

Cómo agregar dispositivos de RAC o grupos de dispositivos de RAC

Para agregar dispositivos de RAC o grupos de dispositivos de RAC:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Escriba el nombre del dispositivo de RAC o del grupo de dispositivos de RAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y luego en **Aceptar**.

Habilitación de SSL en un controlador de dominio

Si está usando la autoridad de certificados raíz de empresa de Microsoft para asignar automáticamente todos controladores de dominio a un certificado SSL, realice los pasos siguientes para habilitar SSL en cada controlador de dominio.

1. Instale una Entidad emisora raíz de la empresa de Microsoft en un controlador de dominio.
 - a. Seleccione **Inicio**→ **Panel de control**→ **Agregar o quitar programas**.
 - b. Seleccione **Agregar o quitar componentes de Windows**.
 - c. En el **Asistente de componentes de Windows**, seleccione la casilla de marcación de **Servicios de certificado**.
 - d. Seleccione **Entidad emisora raíz de la empresa** como **Tipo de entidad emisora de certificados** y haga clic en **Siguiente**.
 - e. Escriba el **Nombre común para esta entidad emisora de certificados**, haga clic en **Siguiente** y haga clic en **Terminar**.
2. Active SSL en cada uno de los controladores de dominio instalando el certificado SSL para cada controlador.
 - a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Directiva de seguridad de dominio**.
 - b. Expanda la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse **Configuración de la petición de certificados automática** y haga clic en **Petición de certificados automática**.
 - c. En **Asistente para instalación de petición automática de certificado**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
 - d. Haga clic en **Siguiente** y haga clic en **Terminar**.

Exportación del certificado de CA de raíz del controlador de dominio

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

1. Localice el controlador de dominio que ejecuta el servicio Microsoft Enterprise CA.
2. Haga clic en **Inicio**→ **Ejecutar**.
3. En el campo **Ejecutar**, escriba `mmc` y haga clic en **Aceptar**.
4. En la ventana **Console 1** (MMC), haga clic en **Archivo** (o **Consola** en los equipos con Windows 2000) y seleccione **Agregar o quitar complemento**.
5. En la ventana **Agregar o quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione la cuenta **Equipo** y haga clic en **Siguiente**.
8. Seleccione **Equipo local** y haga clic en **Terminar**.
9. Haga clic en **Aceptar**.
10. En la ventana **Consola 1**, amplíe la carpeta **Certificados**, amplíe la carpeta **Personal**, y haga clic en la carpeta **Certificados**.
11. Ubique y haga clic con el botón derecho del mouse en el certificado de CA raíz, seleccione **Todas las tareas** y haga clic en **Exportar...**
12. En el **Asistente para exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **X.509 codificado base 64 (.CER)** como formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio en el sistema.
15. Cargue el certificado que guardó en el [paso 14](#) en el DRAC 5.

Para cargar el certificado por medio de RACADM, consulte "[Configuración de los valores de Active Directory del DRAC 5 por medio de RACADM](#)".

Para cargar el certificado por medio de la interfaz basada en web, realice el procedimiento siguiente:

- a. Abra una ventana de un explorador compatible de web.
- b. **Inicie sesión** en la interfaz basada en web del DRAC 5.
- c. **Expanda el árbol de Sistema**, haga clic en **Acceso remoto**.
- d. Haga clic en la ficha **Configuración** y después haga clic en **Seguridad**.
- e. En la página **Menú principal del certificado de seguridad**, seleccione **Cargar certificado del servidor** y haga clic en **Aplicar**.
- f. En la pantalla **Carga del certificado**, realice uno de los procedimientos siguientes:
 - o Haga clic en **Examinar** y seleccione el certificado
 - o En el campo **Valor**, escriba la ruta de acceso al certificado.
- g. Haga clic en **Aplicar**.

Cómo importar el certificado SSL de firmware del DRAC 5

Use el procedimiento siguiente para importar el certificado SSL de firmware del DRAC 5 a todas las listas de certificados confiables del controlador de dominio.

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

 **NOTA:** Si el certificado SSL de firmware del DRAC 5 está firmado por una autoridad de certificados reconocida, no necesita realizar los pasos descritos en esta sección.

El certificado SSL del DRAC 5 es el certificado idéntico que se usa para el Web Server del DRAC 5. Todos los controladores del DRAC 5 se envían con un certificado predeterminado autofirmado.

Para acceder al certificado por medio de la interfaz basada en web del DRAC 5, seleccione **Configuración** → **Active Directory** → **Descargar certificado de servidor del DRAC 5**.

1. En el controlador de dominio, abra una ventana de **Consola de MMC** y seleccione **Certificados** → **Autoridades de certificados raíz de confianza**.
2. Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
3. Haga clic en **Siguiente** y localice el archivo del certificado SSL.
4. Instale el certificado de SSL de RAC en la **Autoridad de certificados raíz de confianza** de cada controlador de dominio.

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

Configuración del DRAC 5

1. Abra una ventana de un explorador compatible de web.
2. Inicie sesión en la interfaz basada en web del DRAC 5.
3. Expanda el árbol de **Sistema**, 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. Seleccione la casilla de marcación **Habilitar Active Directory**.
7. Teclee el **Nombre del DRAC**. Este nombre debe ser el mismo que el nombre común del objeto de RAC que usted creó en el controlador de dominio (consulte el [paso 3](#) de "[Creación de un objeto de dispositivo del RAC](#)").
8. Escriba el **Nombre del dominio raíz**. El **Nombre del dominio raíz** es el nombre del dominio raíz completo del bosque.
9. Escriba el **Nombre del dominio del DRAC** (por ejemplo, drac5.com). No use el nombre de NetBIOS. El **Nombre del dominio del DRAC** es el nombre del dominio completo del subdominio donde se encuentra el objeto de dispositivo de RAC.
10. Escriba el valor de **Tiempo de espera** en segundos.
11. Haga clic en **Aplicar** para guardar la configuración de Active Directory.
12. Haga clic en **Volver al menú principal de Active Directory**.
13. Cargue el certificado raíz de CA del bosque de dominio en el DRAC 5.
 - a. Seleccione la casilla **Cargar certificado de CA de Active Directory** y luego haga clic en **Siguiente**.
 - b. En la página **Carga del certificado**, escriba la ruta de acceso al archivo del certificado o desplácese hasta el archivo del certificado y haga clic en **Aplicar**.

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

Los certificados SSL de los controladores de dominio del bosque de dominio deben haber firmado este certificado de CA raíz. Tenga el certificado de CA raíz disponible en el sistema local (consulte "[Exportación del certificado de CA de raíz del controlador de dominio](#)").

El Web Server del DRAC 5 se reinicia automáticamente después de que se hace clic en **Aplicar**.

14. Cierre sesión y luego inicie sesión en el DRAC 5 para completar la configuración del componente Active Directory del DRAC 5.
15. En el árbol de **Sistema**, haga clic en **Acceso remoto**.
16. Haga clic en la ficha **Configuración** y después haga clic en **Red**.
Aparecerá la página **Configuración de la red**.
17. Si se selecciona **Usar DHCP (para la dirección IP del NIC)** en **Configuración de la red**, entonces seleccione **Usar DHCP para obtener la dirección del servidor DNS**.
Para introducir manualmente una dirección IP de servidor DNS, deseleccione **Usar el DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP primaria y alternativa del servidor DNS.
18. Haga clic en **Aplicar cambios**.
Esto concluye la configuración del componente Active Directory del DRAC 5.

Configuración de los valores de Active Directory del DRAC 5 por medio de RACADM

Utilice los comandos siguientes para configurar el componente Active Directory del DRAC 5 por medio de RACADM en vez de la interfaz basada en web.

1. Abra un símbolo del sistema y escriba los siguientes comandos de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1  
  
racadm config -g cfgActiveDirectory -o cfgADracDomain <nombre del dominio completo del RAC>  
  
racadm config -g cfgActiveDirectory -o cfgADrootDomain <nombre del dominio raíz completo>  
  
racadm config -g cfgActiveDirectory -o cfgADracName <nombre común del RAC>  
  
racadm sslcertupload -t 0x2 -f <certificado de CA raíz de ADS>  
  
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2. Si el DHCP está activado en el DRAC 5 y usted desea usar el DNS proporcionado por el servidor DHCP, escriba lo siguiente:

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

3. Si el DHCP está deshabilitado en el DRAC 5 o si desea introducir manualmente la dirección IP de DNS, escriba lo siguiente:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0  
  
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP primaria de DNS>  
  
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

4. Presione **Entrar** para completar la configuración del componente Active Directory del DRAC 5.

Uso de Active Directory para iniciar sesión en el DRAC 5

Puede usar Active Directory para iniciar sesión en el DRAC 5 por medio de uno de los métodos siguientes:

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

La sintaxis de inicio de sesión es consecuente para los tres métodos:

```
<nombre_de_usuario@dominio>
```

```
o
```

```
<dominio>\<nombre_de_usuario> o <dominio>/<nombre_de_usuario>
```

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

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

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

Preguntas frecuentes

La [tabla 6-8](#) muestra una lista de las preguntas y respuestas frecuentes.

Tabla 6-8. Utilización del DRAC 5 con Active Directory: Preguntas frecuentes

| Pregunta | Respuesta |
|--|--|
| ¿Puedo iniciar sesión en el DRAC 5 utilizando Active Directory entre varios bosques? | El algoritmo de consulta de Active Directory del DRAC 5 sólo admite un solo árbol en un solo bosque. |
| ¿El inicio de sesión en el DRAC 5 mediante Active Directory funciona en el modo mixto (es decir, los controladores de dominio en el bosque ejecutan distintos sistemas operativos, como Microsoft Windows NT® 4.0, Windows® 2000 o Windows Server 2003)? | Sí. En el modo mixto, todos los objetos que el proceso de consulta del DRAC 5 utiliza (entre el usuario, el objeto de dispositivo del RAC y el objeto de asociación) tienen que estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory ampliado por Dell verifica el modo y limita a los usuarios a fin de crear objetos a través de dominios si se encuentra en modo mixto. |
| ¿El uso del DRAC 5 con Active Directory admite varios entornos de dominio? | Sí. El nivel de función del bosque de dominio debe estar en modo Nativo o en modo de Windows 2003. Además, los grupos entre el objeto de asociación, los objetos de usuario del RAC y los objetos de dispositivo del RAC (incluso el objeto de asociación) deben ser grupos universales. |
| ¿Estos objetos ampliados por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes? | El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento de usuarios y equipos de Active Directory extendido de Dell le obliga a crear estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes. |
| ¿Hay alguna restricción para la configuración SSL del controlador de dominio? | Sí. Todos los certificados SSL de los servidores de Active Directory en el bosque deben estar firmados por la misma CA raíz pues el DRAC 5 sólo permite cargar un certificado SSL de CA de confianza. |
| Creé y cargué un nuevo certificado de RAC y ahora la interfaz por web se inicia. | Si usted usa los servicios de certificados de Microsoft para generar el certificado del RAC, una causa probable de esto es que usted por descuido haya elegido Certificado de usuario en vez de Certificado de web cuando creó el certificado. Para recuperarse, cree un nuevo certificado de web desde los Servicios de certificados de Microsoft y cárguelo por medio de RACADM desde el sistema administrado, escribiendo: <pre>racadm sslcertupload -t 0x1 -f <web_sslcert></pre> |
| ¿Qué puedo hacer si no puedo iniciar sesión en el DRAC 5 mediante la autenticación de Active Directory? ¿Cómo soluciono el problema? | <ol style="list-style-type: none">1. Asegúrese de que está usando el nombre del dominio de usuario correcto durante el inicio de sesión y no el nombre de NetBIOS.2. Si tiene una cuenta de usuario de DRAC local, inicie sesión en el DRAC 5 empleando las credenciales locales.3. Después de que haber iniciado sesión, realice los pasos a continuación:<ol style="list-style-type: none">a. Asegúrese de haber seleccionado la casilla Habilitar Active Directory en la página de configuración de Active Directory del DRAC 5.b. Asegúrese que la configuración del DNS sea correcta en la página de configuración de red del DRAC 5.c. Asegúrese de haber cargado en el DRAC 5 el certificado de Active Directory que provino de la autoridad de certificados raíz de Active Directory.d. Revise los certificados de SSL de controlador de dominio para asegurarse que no hayan expirado.e. Asegúrese de que el Nombre del DRAC 5, el Nombre del dominio raíz y el Nombre del dominio del DRAC 5 coincidan con la configuración del entorno de Active Directory. |

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso de la redirección de consola con interfaz gráfica de usuario

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Descripción](#)
- [Uso de redirección de consola](#)
- [Uso de Video Viewer](#)
- [Preguntas frecuentes](#)

Esta sección proporciona información acerca de cómo usar la función de redirección de consola del DRAC 5.

Descripción

La función de redirección de consola del DRAC 5 le permite tener acceso a la consola del servidor local de manera remota en modos de gráficos o de texto. Por medio de la redirección de consola, puede controlar uno o varios sistemas equipados con DRAC 5 desde una ubicación.

Hoy en día, con el poder de formación de redes y la Internet, usted no tiene que sentarse frente a cada servidor para realizar todo el mantenimiento de rutina. Usted puede administrar los servidores desde otra ciudad o incluso desde el otro lado del mundo en su equipo 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** permite administrar el sistema remoto con el teclado, vídeo y mouse en su estación de administración local para controlar los dispositivos correspondientes en un sistema administrado remoto. Esta característica se puede utilizar junto con la característica Medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- 1 Sólo se admiten dos sesiones de redirección de consola simultáneas.
- 1 Las sesiones de redirección de consola sólo pueden estar conectadas a un sistema remoto de destino.
- 1 No se puede configurar una sesión de redirección de consola en el sistema local.
- 1 Se requiere de una amplitud de banda de red mínima disponible de 1 MB/s.

Frecuencias de actualización de las resoluciones de pantalla admitidas en el sistema administrado

La [tabla 7-1](#) muestra una lista de las resoluciones de pantalla admitidas y de las frecuencias de actualización correspondientes para una sesión de redirección de consola que se ejecuta en el sistema administrado.

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

| Resolución de pantalla | Frecuencia 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 el redirección de consola en la estación de administración, realice los procedimientos siguientes:

1. Instale y configure un explorador de web admitido. Consulte las secciones siguientes para obtener más información:
 - o ["Exploradores de web admitidos"](#)
 - o ["Configuración de un explorador de web admitido"](#)
2. Configure la resolución de la pantalla del monitor para que tenga al menos 1280 x 1024 píxeles a 60 Hz con 128 colores. De lo contrario, no podrá ver la consola en **Modo de pantalla completa**.

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. Para obtener más información, consulte "[Cómo acceder a la interfaz basada en web](#)".
2. En el árbol de **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**, use la información en la [tabla 7-2](#) para configurar la sesión de redirección de consola y luego haga clic en **Aplicar cambios**.

Tabla 7-2. Información de la página de configuración de la redirección de consola

| Información | Descripción |
|-------------------------------------|--|
| Activado | Seleccionado = activada; deseleccionado = desactivada |
| Nº máx. de sesiones | Muestra el número de sesiones de redirección de consola disponibles. |
| Sesiones activas | Muestra el número de sesiones activas de redirección de consola. |
| Número de puerto de teclado y mouse | Valor predeterminado = 5900 |
| Número de puerto de vídeo | Valor predeterminado = 5901 |
| Cifrado de vídeo activado | Seleccionado = activado; deseleccionado = desactivado |

Los botones de la [tabla 7-3](#) están disponibles en la página **Configuración de la redirección de consola**.

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

| 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. |

Abrir una sesión de redirección de consola

Cuando abre una sesión de redirección de consola, la aplicación Dell Digital KVM Viewer se inicia y aparece el escritorio del sistema remoto en el visualizador. Al usar la aplicación Digital 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, realice los pasos siguientes.

1. En la estación de administración, abra un explorador de web admitido e inicie sesión en el DRAC 5. Para obtener más información, consulte "[Cómo acceder a la interfaz basada en web](#)".
2. En el árbol de **Sistema**, haga clic en **Sistema**.
3. En la ficha **Consola**, haga clic en **Redirección de consola**.

 **NOTA:** Es posible que aparezca una advertencia de seguridad pidiendo que instale y ejecute complemento de redirección de consola. Verifique la autenticidad del complemento y luego haga clic en **Sí** para instalar y ejecutar el complemento. Si está ejecutando Mozilla Firefox, reinicie el explorador y luego siga en el [paso 1](#).

4. En la página **Redirección de consola**, use la información en la [tabla 7-4](#) para asegurarse que haya una sesión de redirección de consola disponible.

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

| Propiedad | Descripción |
|---------------------------------|---|
| Estado | Conectada o desconectada |
| Nº máx. de sesiones | El número máximo admitido de sesiones de redirección de consola |
| Sesiones activas | El número actual de sesiones activas de redirección de consola |
| Redirección de consola activada | Sí/No |
| Cifrado de vídeo activado | Sí/No |

Los botones de la [tabla 7-5](#) están disponibles en la página **Redirección de consola**.

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

| Botón | Definición |
|------------|---|
| Actualizar | Vuelve a cargar la página Configuración de la redirección de consola |
| Conectar | Abre una sesión de redirección de consola en el sistema remoto de destino. |

5. Si hay una sesión de redirección de consola disponible, haga clic en **Conectar**.

 **NOTA:** Pueden aparecer múltiples casillas de mensaje después de iniciar la aplicación. Para prevenir el acceso no autorizado a la aplicación, se debe navegar a través de estos cuadros de mensajes en tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

 **NOTA:** Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información en la ventana y haga clic en **Sí** para seguir.

La estación de administración se conecta al DRAC 5 y la pantalla de escritorio del sistema remoto aparecerá en la aplicación de visor de KVM digital de Dell.

6. Si dos apuntadores del mouse aparecen 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".

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el sistema remoto que le 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 del mouse e instantáneas. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Cuando comienza 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 correctamente el sistema remoto. Estos ajustes incluyen:

- 1 El acceso a la barra de menú del visor
- 1 El ajuste de la calidad de vídeo
- 1 La sincronización de los apuntadores del mouse

El acceso a la barra de menú del visor

La barra de menú del visor es una barra oculta. Para acceder a la barra de menú, mueva el cursor cerca del borde superior de la pantalla de escritorio del visor.

La barra de menú también puede activarse al presionar la tecla predeterminada de función <F9>. Para reasignar esta tecla de función a una nueva función, realice los pasos a continuación:

1. Presione <F9> o mueva el cursor del mouse hacia la parte superior del Video Viewer.
2. Presione el icono de "tachuela" para hacer que la barra de menú del visor permanezca desplegada.
3. En la barra de menú del visor, haga clic en **Herramientas** y seleccione **Opciones de la sesión**.
4. En la ventana **Opciones de la sesión**, haga clic en la ficha **General**.
5. En la ventana de la ficha **General**, en el cuadro **Pulsación de teclas de activación de menú**, haga clic en el menú desplegable y seleccione otra tecla de función.
6. Haga clic en **Aplicar** y después haga clic en **Aceptar**.

La [tabla 7-6](#) proporciona las principales funciones que se pueden usar en la barra de menú del visor.

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

| Opción del menú | Elemento | Descripción |
|-----------------|---------------------|--|
| Archivo | Capturar en archivo | Captura la pantalla actual del sistema remoto en un archivo .bmp (Windows) o .png (Linux) en el sistema local. Se muestra un cuadro de diálogo que permite guardar el archivo en una ubicación especificada. |

| | | |
|--------------|------------------------------------|---|
| | Salir | Sale de la página Redirección de consola . |
| Ver | Actualizar | Actualiza toda la área de visualización de la pantalla del sistema remoto. |
| | Pantalla completa | Amplía la ventana de la sesión a pantalla completa. |
| Macros | Varios accesos directos de teclado | Ejecuta una combinación de pulsaciones de teclas en el sistema remoto. Para conectar el teclado de la estación de administración al sistema remoto y ejecutar un macro, realice los pasos siguientes: <ol style="list-style-type: none"> 1. Haga clic en Herramientas. 2. En la ventana Opciones de la sesión, haga clic en la ficha General. 3. Seleccione Pasar todas las pulsaciones de teclas al destino. 4. Haga clic en Aceptar. 5. Haga clic en Macros. 6. En el menú Macros, haga clic en una combinación de pulsaciones de tecla para ejecutarla en el sistema de destino. |
| | | |
| Herramientas | Ajuste de vídeo automático | Vuelve a calibrar la salida de vídeo del visor de la sesión. |
| | Ajuste de vídeo manual | Ofrece controles individuales para ajustar manualmente la salida de vídeo del visor de la sesión. NOTA: Al ajustar la posición de centrado horizontal se desincronizarán los apuntadores del mouse. |
| | Opciones de la sesión | Proporciona ajustes adicionales de control del vídeo de la sesión. La ficha Mouse le permite seleccionar el sistema operativo que va a utilizar para optimizar el rendimiento del mouse de redirección de consola. Seleccione Windows , Linux o Ninguno . La ficha General ofrece las opciones siguientes: <ol style="list-style-type: none"> 1 Modo de paso de teclado: seleccione Pasar todas las pulsaciones de teclas al destino para pasar las pulsaciones de teclas de la estación de administración al sistema remoto. 1 Pulsación de teclas de activación de menú: selecciona la tecla de función que activa la barra de menú del visor. La ficha Barra de herramientas le permite ajustar el tiempo de Retardo para ocultar barra de herramientas entre 1 y 10 segundos. |
| Ayuda | N/A | Activa el menú Ayuda . |

El ajuste de la calidad de vídeo

Vídeo Viewer proporciona ajustes de vídeo que le permiten optimizar el vídeo para obtener la mejor vista posible. Haga clic en **Ayuda** para obtener más información.

Para ajustar automáticamente la calidad de vídeo, realice los pasos siguientes:

1. Acceda a la barra de menú del visor. Consulte "[Cómo acceder a la barra de menú del visor](#)".
2. Haga clic en **Herramientas** y seleccione **Ajuste de vídeo automático**.

La calidad del vídeo se vuelve a calibrar y el visor de sesión aparece de nuevo.

Para ajustar manualmente la calidad de vídeo, realice los pasos siguientes:

1. Acceda a la barra de menú del visor. Consulte "[Cómo acceder a la barra de menú del visor](#)".
2. Haga clic en **Herramientas** y seleccione **Ajuste de vídeo manual**.
3. En la ventana **Ajuste de vídeo**, haga clic en cada botón de ajuste de vídeo y cambie los controles según sea necesario.

Cuando ajuste la calidad de vídeo manualmente, observe las siguientes directrices:

- 1 Para evitar que los apuntadores del mouse se desincronicen, ajuste el valor horizontal de manera que la pantalla de escritorio del sistema remoto esté centrado en la ventana de la sesión.
- 1 La reducción a cero del valor de la proporción de ruido de píxeles hace que varios comandos de actualización de vídeo generen un tráfico excesivo de red y que el vídeo parpadee en la ventana de Vídeo Viewer. Dell recomienda que ajuste el valor de la Proporción del ruido de los píxeles a un nivel que proporcione el rendimiento óptimo del sistema y mejore los píxeles, minimizando el tráfico de red.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema PowerEdge remoto que usa la redirección de consola, la velocidad de aceleración del mouse en el sistema remoto puede que no se sincronice con el apuntador del mouse en la estación de administración, haciendo que dos apuntadores de mouse aparezcan en la ventana de Vídeo Viewer.

Para sincronizar los apuntadores del mouse, realice los pasos siguientes:

1. Acceda a la barra de menú del visor. Consulte "[Cómo acceder a la barra de menú del visor](#)".
2. Haga clic en **Herramientas** y seleccione **Opciones de la sesión**.
3. Haga clic en la ficha **Mouse**, seleccione el sistema operativo de la estación de administración y haga clic en **Aceptar**.
4. Haga clic en **Herramientas** y seleccione **Ajuste de vídeo manual**.
5. Ajuste los controles horizontales de manera que la pantalla de escritorio del sistema aparezca en el centro de la ventana de la sesión .
6. Haga clic en **Aceptar**.

Preguntas frecuentes

La [tabla 7-7](#) muestra una lista de preguntas y respuestas frecuentes.

Tabla 7-7. Uso de la redirección de consola: Preguntas frecuentes

| Pregunta | Respuesta |
|---|--|
| Veo distorsiones de vídeo en mi pantalla. ¿Cómo resuelvo este problema? | En la ventana Redirección de consola , haga clic en Actualizar para actualizar la pantalla. NOTA: Es posible que sea necesario hacer clic en Actualizar varias veces para corregir la distorsión de vídeo. |
| Durante la redirección de consola, se bloquearon el teclado y el mouse después de regresar del estado de hibernación en un sistema Windows 2000. ¿Qué causó que esto sucediera? | Para resolver este problema, debe de restablecer el DRAC 5 ejecutando el comando racadm racreset . |
| No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola. | Asegúrese que la resolución del monitor de la estación de administración esté establecida en 1280 x 1024. |
| Durante la redirección de consola, se bloqueó el mouse después de regresar del estado de hibernación en un Windows Server 2003. ¿Por qué sucedió esto? | Para resolver este problema, seleccione un sistema operativo que no sea Windows para la aceleración del mouse del menú desplegable de la ventana KVM virtual (vKVM), espere de 5 a 10 segundos y luego seleccione Windows de nuevo. Si el problema no se resuelve, debe de restablecer el DRAC 5 ejecutando el comando racadm racreset . Si el problema aún no se resuelve, debe de restablecer el DRAC 5 ejecutando el comando racadm racreset hard . |
| ¿Por qué no funcionan el teclado y el mouse del vKVM? | Debe establecer el controlador USB en Activado con compatibilidad del BIOS en la configuración del BIOS del sistema administrado. Reinicie el sistema administrado y presione <F2> para ingresar al programa de configuración. Seleccione Dispositivos integrados y luego seleccione Controlador USB . Guarde los cambios y reinicie el sistema. |
| ¿Por qué aparece una pantalla en blanco en la consola del sistema administrado cuando Windows muestra una pantalla azul? | El sistema administrado no tiene al archivo controlador correcto de vídeo ATI. Debe actualizar el archivo controlador de vídeo por medio del CD <i>Dell PowerEdge Installation and Server Management</i> . |
| ¿Por qué recibo una pantalla en blanco en la consola remota después de completar una instalación de Windows 2000? | El sistema administrado no tiene al archivo controlador correcto de vídeo ATI. La redirección de consola del DRAC 5 no funcionará correctamente con el controlador de vídeo SVGA del CD de distribución de Windows 2000. Debe instalar Windows 2000 con el CD <i>Dell PowerEdge Installation and Server Management</i> para asegurarse de que tiene los archivos controladores admitidos más recientes para 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 al archivo controlador correcto de vídeo ATI. Debe actualizar el archivo controlador de vídeo por medio del CD <i>Dell PowerEdge Installation and Server Management</i> . |
| ¿Por qué aparece una pantalla en blanco en el sistema administrado en la ventana de DOS de pantalla completa en Windows? | El sistema administrado no tiene al archivo controlador correcto de vídeo ATI. Debe actualizar el archivo controlador de vídeo por medio del CD <i>Dell PowerEdge Installation and Server Management</i> . |
| ¿Por qué no puedo ingresar al programa de configuración del BIOS presionando la tecla <F2>? | Esta conducta es usual en un entorno de Windows. Utilice su mouse para hacer clic en el área de la ventana Redirección de consola para ajustar el enfoque. Para llevar el enfoque a la barra de menú de la parte inferior de la ventana de Redirección de consola, use al mouse y haga clic en uno de los objetos en la barra de menú de la parte inferior. |
| ¿Por qué no se sincroniza el mouse del vKVM cuando utilizo el CD <i>Dell PowerEdge Installation and Server Management</i> para instalar el sistema operativo de manera remota? | Configure el redirección de consola para el sistema operativo que se está ejecutando en el sistema de destino. <ol style="list-style-type: none"> 1. En el menú de la barra de herramientas vKVM, haga clic en Herramientas y seleccione Opciones de la 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 está ejecutando en el sistema de destino y haga clic en Aceptar. |
| ¿Por qué no se sincroniza el mouse del vKVM después de regresar de una hibernación en un sistema Windows? | Seleccione un sistema operativo distinto para la aceleración de mouse en el menú desplegable de la ventana del vKVM. Posteriormente, vuelva al sistema operativo original para inicializar el dispositivo de mouse USB. <ol style="list-style-type: none"> 1. En la barra de herramientas vKVM, haga clic en Herramientas y seleccione Opciones de la 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 Aceptar. |

| | |
|---|---|
| | 4. Inicialice el dispositivo de mouse USB. |
| ¿Por qué no se sincroniza el mouse en DOS al realizar una redirección de consola? | El BIOS de Dell emula el archivo controlador del mouse como si fuera un mouse PS/2. Debido a su diseño, el mouse PS/2 usa posiciones relativas para el apuntador del mouse, lo que ocasiona un retraso de la sincronización. El DRAC 5 tiene a un archivo controlador de mouse USB, que habilita la posición absoluta y el seguimiento más cercano del apuntador del mouse. Aun cuando el DRAC 5 pasara la posición absoluta del mouse USB al BIOS de Dell, la emulación del BIOS lo convertiría nuevamente la posición relativa y el comportamiento seguiría siendo el mismo. |
| ¿Por qué el mouse no se sincroniza en la consola de texto de Linux? | El KVM virtual requiere del archivo controlador de mouse USB, pero dicho archivo sólo está disponible en el sistema operativo X Window. |
| Aún tengo problemas con la sincronización del mouse. | Compruebe que la pantalla de escritorio del sistema de destino está centrada en la ventana de redirección de consola. <ol style="list-style-type: none"> 1. En la barra de herramientas vKVM, haga clic en Herramientas y seleccione Ajuste de vídeo manual. 2. Ajuste los controles horizontales y verticales según sea necesario para alinear la pantalla de escritorio en la ventana de redirección de consola. 3. Haga clic en Cerrar. 4. Mueva el cursor del mouse del sistema de destino a la esquina superior izquierda de la ventana de redirección de consola y luego regrese el cursor al centro de la ventana. 5. Repita del paso 2 al paso 4 hasta que ambos cursores estén sincronizados. |
| ¿Por qué no funcionan el mouse y el teclado del vKVM al cambiar la aceleración del mouse para sistemas operativos diferentes? | El teclado y el mouse del vKVM USB se inactivan por 5 ó 10 segundos después de cambiar la aceleración del mouse. Algunas veces, la carga de la red puede hacer que esta operación tome más tiempo de lo normal (más de 10 segundos). |
| ¿Por qué no puedo ver la parte inferior de la pantalla del servidor desde la ventana vKVM? | Asegúrese que la resolución de la pantalla del servidor sea de 1280 x 1024 pixeles a 60 Hz con 128 colores. |
| ¿Por qué no puedo usar un teclado o mouse mientras instalo un sistema operativo Microsoft® de manera remota por medio de la redirección de consola del DRAC5? | Cuando instala de manera remota un sistema operativo Microsoft admitido en un sistema con la redirección de consola habilitada en el BIOS, aparece un mensaje de conexión de EMS que le pide que seleccione Aceptar para poder continuar. Usted no puede usar el mouse para seleccionar Aceptar de manera remota. Debe seleccionar Aceptar en el sistema local o reiniciar el sistema administrado de manera remota, volver a instalar y luego desactivar la redirección de consola en el BIOS. Microsoft genera este mensaje para alertar al usuario que la redirección de consola está activada. Para asegurarse de que este mensaje no aparezca, desactive siempre la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota. |
| ¿Por qué la redirección de consola no muestra el menú de inicio del sistema operativo en las versiones en chino, japonés y coreano de Microsoft Windows 2000? | En sistemas que ejecutan Windows 2000 que se pueden iniciar en varios sistemas operativos, cambie el sistema operativo de inicio predeterminado realizando los pasos siguientes: <ol style="list-style-type: none"> 1. Haga clic con el botón derecho del mouse en el icono Mi PC y seleccione Propiedades. 2. Haga clic en la ficha Avanzado. 3. Haga clic en Inicio y recuperación. 4. Seleccione el nuevo sistema operativo predeterminado en la lista Inicio. 5. En la lista Mostrar para el cuadro, escriba el número de segundos que la lista de opciones debería mostrarse antes de que el sistema operativo predeterminado se inicie automáticamente. |
| ¿Por qué el indicador Bloq Num de mi estación de administración no refleja el estado del Bloq Num en el servidor remoto? | Cuando se accede por medio del DRAC 5, el indicador Bloq Num de la estación de administración no necesariamente coincide con el estado del Bloq Num del servidor remoto. El estado del indicador Bloq Num depende del valor que tenga el servidor remoto cuando la sesión remota está conectada, independientemente del estado del Bloq Num en la estación de administración. |
| ¿Por qué aparecen varias ventanas de Sesión Viewer cuando establezco una sesión de redirección de consola? | Usted está configurando una sesión de redirección de consola para el sistema local. Reconfigure la sesión para 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, ese usuario podrá suprimir las acciones de usted, sin advertencia. |
| ¿Cuánta amplitud de banda necesito para poder ejecutar una sesión de redirección de consola? | Dell recomienda una conexión de 5 MB/s para tener un buen rendimiento. Se requiere una conexión de 1 MB/s para tener el rendimiento mínimo. |
| ¿Cuáles son los requisitos mínimos de sistema para que mi estación de administración pueda ejecutar la redirección de consola? | Se requiere que la estación de administración tenga un procesador Intel Pentium III a 500 MHz con al menos 256 MB de RAM. |
| ¿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. |

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso y configuración de medios virtuales

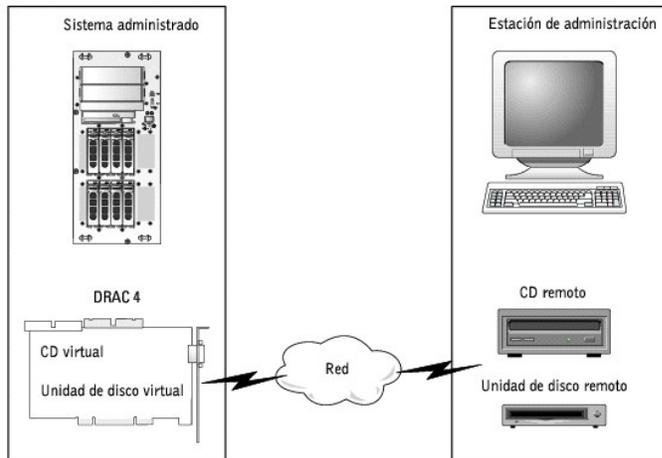
Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Descripción](#)
- [Requisitos del sistema operativo en el sistema administrado](#)
- [Instalación del complemento de medios virtuales](#)
- [Ejecución de los medios virtuales](#)
- [Uso de la unidad flash virtual](#)
- [Uso de la utilidad de interfaz de línea de comandos de los medios virtuales](#)
- [Preguntas frecuentes](#)

Descripción

La función de medios virtuales proporciona al sistema administrado una unidad de CD virtual, que puede usar medios ordinarios de cualquier lugar en la red. La [figura 8-1](#) muestra la arquitectura general de los medios virtuales.

Figura 8-1. Arquitectura general de los 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 equipado con una tarjeta DRAC 5. Las unidades de CD y de disquete 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 BIOS y el sistema operativo del sistema administrado 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 en la red. Cuando se inicia el explorador del RAC por primera vez y se accede a la página de medios virtuales, el complemento de medios virtuales se descarga del Web Server del DRAC 5 y se instala automáticamente en la estación de administración. Para que el componente de medios virtuales funcione correctamente, el complemento de medios virtuales debe estar instalado en la estación de administración.

Cuando los medios virtuales se conectan, todas las solicitudes de acceso a la unidad virtual de CD o de disco provenientes del sistema administrado son dirigidas a la estación de administración por la red. La conexión de los medios virtuales idéntica al proceso de insertar discos en los dispositivos virtuales. Cuando los medios virtuales no están conectados, los dispositivos virtuales en el sistema administrado se comportan como dos unidades sin discos insertados en ellas.

La [tabla 8-1](#) muestra una lista de las conexiones de unidades admitidas para las unidades ópticas y de disco flexible virtuales.

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

Tabla 8-1. Conexiones de unidades admitidas

| Conexiones admitidas de unidades de disco flexible virtuales | Conexiones admitidas de unidades ópticas virtuales |
|---|--|
| Unidad heredada de disco flexible de 1,44 con un disco de 1,44 pulgadas | Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM |
| Unidad de disco flexible USB con un disco de 1,44 pulgadas | Archivo de imagen de CD-ROM en el formato ISO9660 |
| Imagen de disco flexible de 1,44 pulgadas | Unidad USB de CD-ROM con disco CD-ROM. |

Requisitos del sistema operativo en el sistema administrado

Los medios virtuales son compatibles con sistemas que ejecutan los sistemas operativos siguientes:

- 1 Microsoft® Windows 2000 Server con Service Pack 4
- 1 Windows Server™ 2003
- 1 Red Hat Enterprise Linux AS, ES y WS (versión 3.0)
- 1 Red Hat Enterprise Linux AS, ES y WS (versión 4)
- 1 SUSE® Linux Enterprise Server (versión 9) con Service Pack 2 (SP2) para Intel EM64T

Para conocer los sistemas operativos admitidos más recientes, consulte el archivo *Léame* del DRAC 5 y la *Guía de compatibilidad de Dell OpenManage™ Server Administrator*.

Instalación del complemento de medios virtuales

Para poder usar el componente de medios virtuales, el complemento de explorador para medios virtuales debe estar instalado en la estación de administración. Después de que abra la interfaz de usuario del DRAC 5 y abra la página de medios virtuales, el explorador automáticamente descargará el complemento, de ser necesario. Si el complemento se instala correctamente, la página de medios virtuales mostrará una lista de los discos flexibles 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 de ActiveX. Establezca la seguridad del explorador en **Medio** o otro nivel menor para permitir que Internet Explorer descargue e instale los controles firmados de ActiveX.

Para obtener más información, consulte "[Exploradores de web admitidos](#)".

Además, se deben tener derechos de administrador para instalar y usar 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 le muestre una advertencia de seguridad.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Mozilla o Firefox. Si el complemento de medios virtuales no se ha instalado o si hay una versión más reciente disponible, aparecerá un cuadro de diálogo durante el procedimiento de instalación para que confirme la instalación del complemento en la estación de administración. Asegúrese que la identificación del usuario que ejecuta el explorador tenga permisos de escritura en el árbol de directorio del explorador. Si la identificación del usuario no tiene permisos de escritura, no podrá instalar el complemento de medios virtuales.

Para obtener más información, consulte "[Exploradores de web admitidos](#)".

Ejecución de los medios virtuales

 **AVISO:** No ejecute un comando `racreset` cuando esté ejecutando una sesión de medios virtuales. Si lo hace, pueden producirse resultados no deseados, incluso la pérdida de datos.

Con los medios virtuales, puede "virtualizar" una imagen o unidad de disquete, para hacer que una imagen de disquete, una unidad de disquete o una unidad óptica en la consola de administración estén disponibles en el sistema remoto.

Configuraciones admitidas de los medios virtuales

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

Las unidades de disquete admitidas incluyen una imagen de disquete o una unidad disponible de disquete. Las unidades ópticas admitidas incluyen un máximo de una unidad óptica disponible o un archivo de imagen ISO.

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

Conexión de los medios virtuales

1. Abra un explorador de web admitido en la estación de administración. Consulte "[Exploradores de web admitidos](#)".
2. Conéctese e inicie sesión en el DRAC 5. Para obtener más información, consulte "[Cómo acceder a la interfaz basada en web](#)".
3. Haga clic en la ficha **Medios** y después haga clic en **Medios virtuales**.

Aparecerá la página **Medios virtuales** mostrando las unidades de cliente que pueden ser virtualizadas.

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

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

4. Si se le pide, siga las instrucciones en la pantalla para instalar el complemento de medios virtuales.
5. En el cuadro **Atributo**, realice los pasos siguientes:
 - a. En la columna **Valor**, asegúrese que el valor de estado de **Conectar/Desconectar** sea **Conectado**.
Si el valor es **Desconectado**, realice los pasos siguientes:
 - o En la ficha **Medios**, haga clic en **Configuración**.
 - o En la columna **Valor**, asegúrese que la casilla **Conectar medios virtuales** esté seleccionada.
 - o Haga clic en **Aplicar cambios**.
 - o En la ficha **Medios virtuales**, haga clic en **Medios virtuales**.
 - o En la columna **Valor**, asegúrese que el valor de estado de **Conectar/Desconectar** sea **Conectado**.
 - b. Asegúrese que el valor de **Estado actual** sea **No conectado**. Si el campo **Valor** muestra que está conectado, deberá desconectarse de la imagen o de la unidad antes volver a conectarse.
 - c. 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** o **Archivo de imagen ISO** e introduzca o desplácese hasta el archivo de imagen que desea virtualizar.

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

7. Haga clic en **Conectar**.

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

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

Desconexión de los medios virtuales

Haga clic en **Desconectar** para desconectar todas las imágenes y unidades virtualizadas de la estación de administración. **Todas** las imágenes o unidades virtualizadas que sean desconectadas ya no estarán disponibles en el sistema administrado.

Cómo conectar y desconectar la función de medios virtuales

El componente de medios virtuales del DRAC 5 está basado en la tecnología USB y puede aprovechar las características "Plug and Play" de USB. El DRAC 5 ofrece también la opción de conectar y desconectar los dispositivos virtuales a partir del bus USB. Cuando los dispositivos se desconectan, el sistema operativo o el BIOS no pueden detectar la conexión de ninguna unidad. Cuando los dispositivos virtuales se conectan, las unidades son visibles. A diferencia del DRAC 4, en donde las unidades sólo podían activarse o desactivarse en el siguiente inicio de sistema, los dispositivos virtuales del DRAC 5 pueden ser conectados o desconectados en cualquier momento.

Los dispositivos virtuales se pueden conectar o desconectar por medio de un explorador de web, racadm local, racadm remoto, Telnet y puerto serie. Para conectar o desconectar los medios virtuales usando un explorador de web, diríjase a la página de medios y después a la página de configuración de medios; ahí puede cambiar los valores y aplicarlos.

Conexión de los medios virtuales por medio de RACADM

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

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

Desconexión de los medios virtuales por medio de RACADM

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

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

Inicio a partir de los medios virtuales

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

Para cambiar el valor en el BIOS, realice los pasos a continuación:

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

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

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

El sistema administrado se reinicia.

El sistema administrado intenta iniciarse a partir de un dispositivo iniciable con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio iniciable está presente, el sistema se inicia a partir del dispositivo virtual. De lo contrario, el sistema ignora el dispositivo, como en el caso de un dispositivo físico sin medios iniciables.

Instalación de sistemas operativos mediante los medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas para concluir. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de los medios virtuales puede tardar menos de 15 minutos para concluir. Para obtener más información, consulte "[Instalación del sistema operativo por medio de VM-CLI](#)".

1. Verifique lo siguiente:
 - 1 El CD de instalación del sistema operativo está insertado en la unidad de CD de la estación de administración.
 - 1 La unidad local de CD está seleccionada.
 - 1 Está conectado a las unidades virtuales.
2. Siga los pasos de la sección "[Inicio a partir de los medios virtuales](#)" para iniciar a partir de los medios virtuales y asegurar que el BIOS esté configurado para iniciarse a partir de la unidad de CD desde la que se realiza la instalación.
3. Siga las instrucciones en la pantalla para completar la instalación.

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

Sistemas con Windows

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

El uso de las unidades virtuales en el entorno de Windows es similar al uso de las unidades físicas. Cuando se conecta a los medios en una estación de administración, el medio está disponible en el sistema cuando se hace clic en el unidad y se examina su contenido.

Sistemas con Linux

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

Uso de la unidad flash virtual

El DRAC 5 proporciona una unidad virtual de 16 MB de memoria flash persistente que residen en el sistema de archivos de éste y que puede usarse como almacenamiento persistente al que el sistema tiene acceso. Cuando se activa, la unidad flash virtual se configura como una tercera unidad virtual y aparece en el orden de inicio del BIOS, lo que permite que un usuario inicie a partir de la unidad flash virtual.

 **NOTA:** Para iniciar la unidad flash virtual, la imagen de unidad flash virtual deberá ser una imagen iniciable.

A diferencia de una unidad de CD o de disco flexible que requiere una conexión de cliente externa o un dispositivo funcional en el sistema host, la implantación de una unidad flash virtual sólo requiere del componente de unidad flash virtual persistente del DRAC 5. Los 16 MB de memoria flash aparecen como un unidad USB extraíble y no formateada en el entorno de host.

Use las siguientes directrices al implantar la unidad flash virtual:

- 1 La conexión o desconexión de la unidad flash virtual produce una nueva numeración de USB, lo cual conecta y desconecta todos los dispositivos de medios virtuales, respectivamente (por ejemplo, la unidad de CD y la unidad de disco flexible).
- 1 Cuando activa o desactiva la unidad flash virtual, el estado de la conexión de la unidad de CD o de disquete de los medios virtuales no cambia.

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

Activación de la unidad flash virtual

Para activar la unidad flash virtual, abra un ventana de símbolo de sistema, escriba el comando siguiente y presione <Entrar>:

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

Desactivación de la unidad flash virtual

Para desactivar la unidad flash virtual, abra un ventana de símbolo de sistema, escriba el comando siguiente y presione <Entrar>:

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

Cómo guardar imágenes en una unidad flash virtual

La unidad flash virtual se puede formatear desde el host administrado. Si está ejecutando el sistema operativo Windows, haga clic con el botón derecho del mouse y seleccione **Formatear**. Si está ejecutando Linux, las herramientas de sistema como **format** y **fdisk** le permiten particionar y formatear el USB.

Antes de cargar la imagen del explorador de web del RAC a la unidad flash virtual, asegúrese que el archivo de imagen tiene un tamaño de entre 1,44 MB y 16 MB (incluyendo estos límites) y que la unidad flash virtual está desactivada. Después de descargar la imagen y de volver a activar la unidad flash virtual, el sistema y el BIOS reconocerán dicha unidad.

Configuración de una unidad flash virtual iniciable

1. Inserte un disco iniciable en la unidad de disco flexible o inserte un CD iniciable en la unidad óptica.
2. Reinicie el sistema e inicie la unidad seleccionada.
3. Agregue una partición a la unidad flash virtual y habilite la partición.

Si la unidad flash virtual está emulando el disco duro, use **fdisk**. Si la unidad flash virtual está configurada como la unidad B:, emulará un disco flexible y no se necesitará de una partición para configurar la unidad flash virtual como unidad iniciable.

4. Usando el comando **format**, formatee la unidad con la opción **/s** para transferir los archivos de sistema a la unidad flash virtual.

Por ejemplo:

```
format /s x
```

donde *x* es la letra de unidad que está asignada a la unidad flash virtual.

5. Apague el sistema y retire el disco o CD iniciable de la unidad correspondiente.
6. Encienda el sistema y verifique que éste se inicie a partir de la unidad flash virtual y con la petición 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 medios virtuales (VM-CLI) es una interfaz de línea de comandos compatible con el uso de secuencias de comandos que ofrece las funciones de medios virtuales de la estación de administración al DRAC 5 en el sistema remoto.

La utilidad VM-CLI ofrece las siguientes características:

- 1 Admite varias sesiones activas al mismo tiempo.

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

- 1 Los dispositivos de medios extraíbles o los archivos de imagen que sean consecuentes con los complementos de medios virtuales
- 1 Terminación automática cuando la opción "iniciar una vez" del firmware del DRAC está activada.
- 1 Comunicaciones seguras con el DRAC 5 por medio de la Capa de conexión segura (SSL)

Antes de ejecutar la utilidad, compruebe que cuenta con privilegio de usuario de medios virtuales para el DRAC 5 en el sistema remoto.

Si el sistema operativo admite los privilegios de administrador o una pertenencia a grupos o privilegio específico del sistema operativo, también deberá tener privilegios de administrador para poder ejecutar el comando VM-CLI.

El administrador del sistema cliente controla los privilegios y los grupos de usuarios, de manera que también controla qué usuarios que pueden ejecutar la utilidad.

Para sistemas Windows, se deben tener privilegios de usuario avanzado para poder ejecutar la utilidad VM-CLI.

En los sistemas Linux, se puede acceder a la utilidad VM-CLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando constituye un medio centralizado para ofrecer acceso sin privilegios administrativos y lleva un registro de todos los comandos de usuario. Para agregar o editar usuarios en el grupo VM-CLI, el administrador usa el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de VM-CLI (o a la secuencia de comandos de VM-CLI) a fin de obtener acceso al DRAC 5 en el sistema remoto y ejecutar la utilidad.

Sistemas operativos admitidos

La utilidad VM-CLI es compatible con los siguientes sistemas operativos:

- 1 Windows XP
- 1 Windows 2000 Server con Service Pack 4
- 1 Windows Server 2003
- 1 Windows Server 2003 R2
- 1 Red Hat Enterprise Linux AS/ES (versión 3)
- 1 Red Hat Enterprise Linux AS/ES (versión 4)
- 1 SUSE Linux Enterprise Server versión 9 con Service Pack 2 para EM64T

Para ver la información más reciente, consulte el archivo *Léame* del DRAC 5 y la *Guía de compatibilidad de Dell OpenManage™ Server Administrator* que se encuentra en el sitio web de asistencia Dell Support en support.dell.com.

Instalación de la utilidad

La utilidad VM-CLI se encuentra en el CD *Dell OpenManage™ Systems Management Consoles* que viene incluido en el paquete de software Dell OpenManage System Management. Para instalar la utilidad, inserte el CD *System Management Consoles* en la unidad de CD del sistema y siga las instrucciones que aparecen en la pantalla.

El CD *System Management Consoles* contiene los productos de software de administración de sistemas más recientes, incluso los diagnósticos, Storage Management, el servicio de acceso remoto y la utilidad RACADM. Este CD también contiene los archivos léame, que proporcionan la información más reciente del producto de software de administración de sistemas.

Además, el CD *Systems Management Consoles* incluye el archivo **vmdeploy**; una secuencia de comandos de muestra que ilustra cómo usar 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 VM-CLI](#)".

Opciones de la línea de comandos

La interfaz 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, una opción para especificar la dirección IP de DRAC 5 requiere la misma sintaxis tanto para la utilidad RACADM como para la utilidad VM-CLI.

El formato del comando de VM-CLI es de la siguiente manera:

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

Toda la sintaxis de la línea de comandos distingue entre mayúsculas y minúsculas. Para obtener más información, consulte "[Parámetros de VM-CLI](#)".

Si el sistema remoto acepta los comandos y el DRAC 5 autoriza la conexión, el comando sigue ejecutándose hasta que se presente cualquiera de los siguientes casos:

- 1 La conexión de VM-CLI termina por algún motivo.
- 1 El proceso es finalizado manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, puede usar el Administrador de tareas para finalizar el proceso.

Parámetros de VM-CLI

Dirección de IP de DRAC 5

`-r <Dirección_IP_de_RAC>[:<puerto_SSL_de_RAC>]`

donde `<Dirección_IP_de_RAC>` es una dirección IP válida y única, o bien, el nombre de Sistema dinámico de nombres de dominio (DDNS) del DRAC 5 (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 una dirección IP o nombre de DDNS no válidos, aparecerá un mensaje de error y el comando finalizará.

Si se omite `<puerto_SSL_de_RAC>`, se utilizará el puerto 443 (predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado del DRAC 5.

Nombre de usuario de 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 atributos siguientes:

- 1 Nombre de usuario válido
- 1 Permiso de usuario de medios virtuales del DRAC

Si la autenticación del DRAC 5 falla, aparecerá un mensaje de error y se finalizará el comando.

Contraseña de usuario de DRAC

`-p <contraseña_de_usuario_del_DRAC>`

Este parámetro proporciona la contraseña para el usuario de DRAC 5 especificado.

Si la autenticación de DRAC 5 falla, se muestra un mensaje de error y se finaliza el comando.

Dispositivo de disco o archivo de Imagen

`-f {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde `<nombre_de_dispositivo>` es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido, incluyendo el número de partición del sistema de archivos montable, si se aplica (para sistemas Linux); y `<archivo_de_imagen>` es el nombre y la ruta de acceso de un archivo de imagen válido.

Este parámetro especifica el dispositivo o el archivo a suministrar los medios virtuales de disco.

Por ejemplo, un archivo de imagen se especifica como:

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

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

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

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`-f /dev/sdb4 # 4th partition on device/dev/sdb` (sistema Linux)

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

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

Dispositivo de CD/DVD o archivo de imagen

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde `<nombre_de_dispositivo>` es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de dispositivo CD/DVD válido (sistemas Linux) y `<archivo_de_imagen>` es el nombre de archivo y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o el archivo que ofrecerá los medios de CD/DVD-ROM virtuales:

Por ejemplo, un archivo de imagen se especifica como:

```
-c c:\temp\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 comandos si no va a virtualizar discos CD o DVD. Si se descubre un valor no válido, un mensaje de error es puesto en la lista y el comando se finaliza.

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

Para mostrar la versión

```
-v
```

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

Para mostrar la ayuda

```
-h
```

Este parámetro muestra un resumen de los parámetros de la utilidad VM-CLI. Si no se proporciona ninguna otra opción que no sea de interruptor, el comando se finaliza sin errores.

Datos cifrados

```
-e
```

Cuando se incluya este parámetro en la línea de comandos, VM-CLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el DRAC 5 en el sistema remoto. Si no se incluye este parámetro en la línea de comandos, la transferencia de datos no se cifrará.

Opciones de núcleo de sistema operativo de VM-CLI

Las siguientes funciones del sistema operativo pueden ser usadas en la línea de comandos de VM-CLI:

- 1 `stderr/stdout` redirection: redirige los mensajes impresos de salida de la utilidad hacia un archivo.

Por ejemplo, al utilizar el carácter mayor que (`>`), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad VM-CLI.

 **NOTA:** La utilidad VM-CLI no lee en la entrada estándar (`stdin`). Por consiguiente, no se requiere la redirección de `stdin`.

- 1 **Ejecución en segundo plano:** de manera predeterminada, la utilidad VM-CLI se ejecuta en primer plano. Use las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en segundo plano. Por ejemplo, en un sistema operativo Linux, el carácter de y comercial (`&`) después del comando hace que el programa sea iniciado como un nuevo proceso de segundo plano.

La técnica última es útil en programas de secuencias de comandos, ya que permite que la secuencia de comandos proceda después de que un nuevo proceso es comenzado para el comando VM-CLI (de otra manera, la secuencia de comandos permanecería bloqueada hasta que el programa VM-CLI sea finalizado). Cuando instancias múltiples de VM-CLI son iniciadas de esta manera, y una o varias de las instancias de comando son finalizadas manualmente, utilice las instalaciones específicas del sistema operativo para listar y finalizar procesos.

Códigos de retorno de VM-CLI

0 = ningún error

1 = No se pudo conectar

2 = Error de línea de comandos de VM-CLI

3 = se perdió la conexión de firmware de RAC

Los mensajes de texto únicamente en inglés también se envían a los mensajes de error estándares siempre que se encuentren errores.

Preguntas frecuentes

La [tabla 8-2](#) muestra una lista de preguntas y respuestas frecuentes.

Tabla 8-2. Uso de los medios virtuales: Preguntas frecuentes

| Pregunta | Respuesta |
|---|---|
| ¿Qué sistemas operativos son compatibles con el DRAC 5? | Consulte " Sistemas operativos admitidos " para obtener una lista de sistemas operativos compatibles. |
| ¿Qué exploradores de web son compatibles con el DRAC 5? | Consulte " Exploradores de web admitidos " para ver una lista de los exploradores de web admitidos. |
| ¿Por qué pierdo a veces mi conexión de cliente? | Algunas veces, usted puede perder su conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si usted cambia el CD en la unidad de CD del sistema cliente, el nuevo CD podría tener una función de ejecución automática. Si es así, el firmware puede agotar el tiempo de espera y la conexión puede perderse si el sistema cliente también tarda mucho en estar listo para leer el CD. Si una conexión se pierde, vuelva a conectarse a partir de la interfaz gráfica de usuario y siga con la operación anterior. |

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso de la interfaz de línea de comandos de RACADM

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

- [Uso de una consola Telnet o serie](#)
- [Uso de RACADM](#)
- [Configuración de varias tarjetas DRAC 5](#)
- [Uso de la utilidad RACADM para configurar el DRAC 5](#)
- [Preguntas frecuentes](#)

La consola serie/Telnet/SSH proporciona un conjunto de comandos RACADM. Los comandos de racadm proporcionan acceso a las funciones de texto compatibles con la interfaz basada en web del DRAC 5.

La utilidad RACADM le permite configurar y administrar de manera local o remota el DRAC 5. RACADM se ejecuta en la estación de administración y en el sistema administrado. RACADM viene incluido en el CD *Dell Systems Management Consoles*.

Puede usar la utilidad RACADM para escribir secuencias de comandos que configurarán varios DRAC 5 automáticamente. Para obtener más información sobre cómo configurar varios DRAC 5, consulte "[Configuración de varias tarjetas DRAC 5](#)".

Esta sección ofrece la información siguiente:

1. Uso de comandos **serie** y **racadm**. Consulte "[Uso de una consola serie o Telnet](#)" o "[Uso de RACADM](#)".
1. Configuración del DRAC5 por medio del comando **racadm**
1. Uso del archivo de configuración de racadm para configurar varias tarjetas DRAC 5

Uso de una consola Telnet o serie

Puede ejecutar los comandos serie de la [tabla 9-1](#) de manera remota por medio de RACADM o desde la petición de comandos de la consola serie, Telnet o SSH.

Conexión con el DRAC 5

Una vez configurado el software de emulador de terminal de la 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 pulse <Entrar>.

Ya está conectado con el DRAC 5.

Inicio de una consola de texto

Una vez que haya iniciado sesión en el DRAC 5 mediante el software de terminal de la estación de administración con Telnet o con SSH, puede redirigir la consola de texto del sistema administrado con el comando **connect com2**, que es un comando Telnet o SSH. Sólo se admite un cliente de **connect com2** a la vez.

Para conectarse a la consola de texto del sistema administrado, abra una ventana de símbolo de sistema del DRAC 5 (que aparece a través de una sesión Telnet o SSH) y escriba:

```
connect com2
```

Usted puede conectarse a la consola serie del sistema administrado desde una sesión serie al presionar <Esc><Mayús><Q>; esto conecta el puerto serie del sistema administrado directamente al puerto COM2 de los servidores y evita 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 historia serie antes de esperar datos del teclado o nuevos caracteres del puerto serie.

 **NOTA:** Cuando use la opción `-h`, los tipos de emulación de terminal del servidor y del cliente (ANSI o VT100) deben ser idénticos; de lo contrario, el mensaje de salida puede aparecer ilegible. Además, establezca la fila de terminal del cliente en 25.

El tamaño predeterminado (y máximo) búfer de historial es de 8192 caracteres. Usted puede definir este número en un valor menor por medio del comando:

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

Uso de RACADM

Usted puede ejecutar los comandos RACADM de forma local o remota desde la petición de comandos de la consola Telnet o serie o mediante una petición de

comandos normal.

Utilice el comando **racadm** para configurar las propiedades del DRAC 5, realizar tareas de administración remota o recuperar un sistema bloqueado.

Para mostrar la lista de subcomandos de **racadm** por medio de **RACADM**, escriba:

```
racadm help
```

La lista de subcomandos incluye todos los comandos compatibles con el DRAC 5.

Sin opciones, el comando **racadm** muestra la información de uso general. Escriba `racadm help` para mostrar una lista de todos los subcomandos disponibles. Escriba `racadm help <subcomando>` para mostrar una lista de la sintaxis y las opciones de línea de comandos del subcomando.

Las siguientes secciones proporcionan información acerca de cómo usar los comandos **racadm**.

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 la configuración del DRAC 5 y una lista de documentos relacionados, consulte "[Instalación y configuración 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, necesita un nombre de usuario (opción -u) y una contraseña (opción -p) válidos, así como la dirección IP del DRAC 5.

 **NOTA:** La capacidad de RACADM remoto es compatible únicamente con las estaciones de administración que ejecutan los sistemas operativos Windows 2000 Server, Windows XP Professional, Windows 2000 Professional, Windows Server 2003, Windows Server 2003 R2, Red Hat Enterprise Linux (versiones 3 y 4) y Linux SUSE.

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 ha sido cambiado por un puerto personalizado diferente al puerto predeterminado (443), se deberá utilizar la siguiente sintaxis:

```
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 9-1](#) muestra una lista de las opciones del comando **racadm**.

Tabla 9-1. Opciones del comando **racadm**

| Opción | Descripción |
|--|--|
| -r <Direc_IP_del_RAC> | Especifica la dirección IP remota del controlador. |
| -r <Direc_IP_del_RAC>:<número de puerto> | Use :<número_de_puerto> si el número de puerto del DRAC 5 no es el puerto predeterminado (443) |
| -i | Le 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 autenticar la transacción del comando. Si se usa la opción -u, se debe usar la opción -p y no se permite la opción -i (interactiva). |
| -p <contraseña> | Especifica la contraseña usada para autenticar la transacción del comando. Si se usa la opción -p, no se permite la opción -i. |

Activación y desactivación de la capacidad de RACADM remota

 **NOTA:** Se recomienda ejecutar estos comandos en el sistema local.

La capacidad remota de RACADM está activada de manera predeterminada. Si está desactivada, escriba el comando siguiente 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 9-2](#) proporciona una descripción de cada subcomando **racadm** que usted puede ejecutar en RACADM. Para obtener un listado detallado de los subcomandos de **racadm**, incluso la sintaxis y las anotaciones válidas, consulte las "[Descripción de subcomandos de RACADM](#)".

Al escribir un subcomando de RACADM, preceda el comando con **racadm**. Por ejemplo:

```
racadm help
```

Tabla 9-2. Subcomandos de RACADM

| Comando | Descripción |
|---|---|
| help | Enumera los subcomandos del DRAC 5. |
| help <subcomando> | Muestra la información sobre el uso del subcomando especificado. |
| arp | Muestra el contenido de la tabla ARP. Las anotaciones en la tabla del ARP no se pueden agregar ni eliminar. |
| clearasrscreen | Borra la última pantalla (de bloqueo) ASR (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 de configuración actuales del RAC. |
| coredump | Muestra el último volcado central del DRAC 5. |
| coredumpdelete | Borra el volcado central almacenado 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 y del sistema del RAC 5. |
| getractive | Muestra la hora del DRAC 5. |
| ifconfig | Muestra la configuración IP actual del RAC. |
| netstat | Muestra la tabla de encaminamiento 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. |
| setniccfa | Establece la configuración IP para el controlador. |
| getniccfa | Muestra la configuración IP actual del controlador. |
| getsvctag | Muestra las etiquetas de servicio. |
| racdump | Vacía información del estado y la condición del DRAC 5 para la depuración de errores. |
| racreset | Restablece el DRAC 5. |
| racresetcfa | Restablece el DRAC 5 a la configuración predeterminada. |
| serveraction | Realiza operaciones de administración de alimentación en el sistema administrado. |
| getraclog | Muestra el registro del RAC. |
| clrsl | Borra las anotaciones del registro de sucesos del sistema. |
| gettracelog | Muestra del registro de rastreo del DRAC 5. Si se usa con -i, el comando muestra el número de anotaciones en el registro de rastreo del DRAC 5. |
| sslcsrgen | Genera y descarga la CSR de la SSL. |
| sslcertupload | Carga un certificado CA o un certificado de servidor en el DRAC 5. |
| sslcertdownload | Descarga un certificado de CA. |
| sslcertview | Muestra un certificado CA o un certificado de servidor en el DRAC 5. |
| testemail | Obliga al DRAC 5 a enviar un correo electrónico a través del NIC del DRAC 5. |
| testtrap | Obliga al DRAC 5 a enviar un SNMP a través del NIC del DRAC 5. |
| vmdisconnect | Obliga a una conexión de medios virtuales a cerrarse. |
| vmkey | Restablece el tamaño de la unidad flash virtual asignándole el tamaño predeterminado (16 MB). |

Mensajes de error de RACADM

Para obtener información acerca de los mensajes de error de la CLI de racadm, consulte "[Preguntas frecuentes](#)" en este capítulo.

Configuración de varias tarjetas DRAC 5

Por medio de RACADM, usted puede configurar una o varias tarjetas DRAC 5 con propiedades idénticas. Cuando realiza una consulta en una tarjeta DRAC 5 específica utilizando las identificaciones de grupo y de objeto de la misma, RACADM crea el archivo de configuración `racadm.cfg` a partir de la información obtenida. Al exportar el archivo a una o varias tarjetas DRAC 5, usted puede configurar los controladores con propiedades idénticas en lapso mínimo de tiempo.

 **NOTA:** Algunos archivos de configuración contienen información exclusiva del DRAC 5 (como 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 procedimientos siguientes:

1. Use RACADM para hacer una consulta en la DRAC 5 de destino que contiene la configuración adecuada.

 **NOTA:** El archivo `.cfg` generado no contiene contraseñas de usuario.

Abra un ventana de símbolo de sistema y escriba:

```
racadm getconfig -f myfile.cfg
```

 **NOTA:** El redireccionamiento de la configuración del RAC hacia un archivo por medio de `getconfig -f` sólo se admite con las interfaces de RACADM local y remoto.

2. Modifique el archivo de configuración usando un editor de textos simple (opcional).
3. Use 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 es necesario, puede configurar el archivo con otro nombre.

Puede usar el comando `getconfig` para realizar las acciones siguientes:

1. Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice)
1. Mostrar todas las propiedades de configuración para un usuario, por nombre de usuario

El subcomando `config` carga la información en otros DRAC 5. Use `config` para sincronizar la base de datos de usuarios y contraseñas con Server Administrator

El usuario elige el nombre del archivo de configuración inicial, `racadm.cfg`. En el ejemplo a continuación, el archivo de configuración se llama `mi_archivo.cfg`. Para crear este archivo, escriba el siguiente comando en el símbolo del sistema:

```
racadm getconfig -f myfile.cfg
```

 **AVISO:** Se recomienda que edite este archivo con un editor de textos simple. La utilidad `racadm` usa un analizador de textos ASCII. Los formatos confunden al analizador, lo cual puede dañar la base de datos de `racadm`.

Creación de un archivo de configuración del DRAC 5

El archivo de configuración de DRAC 5 `<nombre_de_archivo>.cfg` se usa con el comando `racadm config -f <nombre_de_archivo>.cfg`. El archivo de configuración es un archivo de texto simple que permite al usuario crear un archivo de configuración (similar al archivo `.ini`) y configurar el DRAC 5 a partir de este archivo. Se puede usar cualquier nombre de archivo y el archivo no requiere de la extensión `.cfg` (aunque en este apartado se haga referencia al mismo con esa denominación).

El archivo `.cfg` puede ser:

1. Creado
1. Obtenido a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg`
1. Obtenido a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg`, y luego editado

 **NOTA:** Consulte "[getconfig](#)" para obtener información acerca del comando `getconfig`.

El archivo `.cfg` es el primero que se analiza para verificar que los nombres válidos de objeto y de grupo estén presentes y que algunas simples reglas de sintaxis se cumplan. 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 se analiza en su totalidad para asegurar que esté correcto y se muestran todos los errores. Los comandos de escritura no se transmiten al DRAC 5 si se encuentra un error en el archivo `.cfg`. El usuario debe corregir *todos* los errores antes de que tenga lugar cualquier configuración. La opción `-c` se puede usar en el subcomando `config` que verifica sólo la sintaxis y *no* realiza escrituras en el DRAC 5.

Use las pautas siguientes cuando cree un archivo `.cfg`:

1. Si el analizador encuentra un grupo indexado, el valor del objeto delimitado será el que distinga entre los diversos índices.

El analizador lee en todos los índices del DRAC 5 para ese grupo. Los objetos dentro de dicho grupo son modificaciones simples cuando se configura el DRAC 5. Si un objeto modificado representa un índice nuevo, el índice se crea en el DRAC 5 durante la configuración.

- 1 El usuario no puede especificar un índice deseado en un archivo `.cfg`.

Los índices se pueden crear y borrar, de manera que con el tiempo, es posible que el grupo se vaya fragmentando con índices usados y sin usar. Si hay un índice presente, éste se modifica. Si no hay un índice presente, se usará el primer índice disponible. Este método ofrece flexibilidad al momento de agregar anotaciones indexadas en las que el usuario no tiene que hacer coincidencias exactas de índice entre todos los RAC que se están administrando. Los nuevos usuarios se agregan al primer índice disponible. Es posible que un archivo `.cfg` que se analiza y se ejecuta correctamente en un DRAC 5 no funcione correctamente en otro si todos los índices están llenos y usted tiene que agregar un nuevo usuario.

- 1 Use el subcomando `racresetcfg` para configurar todas las tarjetas DRAC 5 con propiedades idénticas.

Use el subcomando `racresetcfg` para volver a establecer los valores originales del DRAC 5 y luego ejecute el comando `racadm config -f <nombre_de_archivo>.cfg`. Asegúrese de que el archivo `.cfg` incluya todos los objetos, usuarios, índices y otros parámetros deseados.

- ➔ **AVISO:** Use el subcomando `racresetcfg` para restablecer la base de datos y la configuración de la tarjeta de interfaz de red del DRAC 5 en sus valores predeterminados originales y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario raíz está disponible, la configuración de los demás usuarios también se restablece en sus valores predeterminados.

Reglas de análisis

- 1 Todas las líneas que comiencen con '#' reciben el tratamiento de comentarios.

Una línea de comentario *debe* iniciar en la columna uno. Un carácter '#' que esté en cualquier otra columna será tratado como carácter '#'.

Algunos parámetros de módem pueden incluir caracteres '#' en la cadena. No se requiere un carácter de escape. Es posible que desee generar un archivo `.cfg` a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y luego realizar un comando `racadm config -f <nombre_de_archivo>.cfg` para otro DRAC 5, sin agregar caracteres de escape.

Ejemplo:

```
#
# This is a comment (Esto es un comentario)

[cfgUserAdmin]

cfgUserAdminPageModemInitString=<Inicio de módem # no es un comentario>
```

- 1 Todas las anotaciones de grupo deben estar encerradas en los caracteres "[" y "]".

El carácter inicial "[" que denota un nombre de grupo *debe* iniciar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquier objeto en dicho grupo. Los objetos que no incluyan un nombre de grupo asociado generarán un error. La información de configuración está organizada en grupos, como se define en "[Definiciones de grupos y objetos de la base de datos de propiedades del DRAC 5](#)".

El ejemplo siguiente muestra un nombre de grupo, objeto y el valor de la propiedad del objeto.

Ejemplo:

```
[cfgLanNetworking] -{nombre de grupo}

cfgNicIpAddress=143.154.133.121 {nombre de objeto}
```

- 1 Todos los parámetros se especifican como pares "objeto=valor" sin espacio en blanco entre el objeto, el signo "=" o el valor.

Los espacios en blanco que se incluyen después del valor se ignoran. Un espacio en blanco dentro de una cadena de valores se deja sin modificación. Cualquier carácter a la derecha del signo '=' se toma tal cual es (por ejemplo, un segundo '=' o un '#', '[', ']', etc.). Estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

Consulte el ejemplo en el boletín anterior.

- 1 El analizador de `.cfg` ignora una anotación de objeto de índice.

El usuario *no puede* especificar el índice que se usa. Si el índice ya existe, se está usando, o bien, la nueva anotación se crea en el primer índice disponible para ese grupo.

El comando `racadm getconfig -f <nombre_de_archivo>.cfg` coloca un comentario frente a los objetos del índice, lo que permite al usuario ver los comentarios que se incluyen.

- 📌 **NOTA:** El usuario puede crear manualmente un grupo indexado por medio del siguiente comando:
`racadm config -g <nombre_de_grupo> -o <objeto_anclado> -i <índice 1-16> <nombre_único_de_ancla>`

- 1 La línea para un grupo indexado *no se puede* borrar de un archivo `.cfg`.

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

```
racadm config -g <nombre de grupo> -o <nombre de objeto> -i <índice 1-16> ""
```

- 📌 **NOTA:** Una cadena NULA (que se identifica por dos caracteres "") indica al DRAC 5 que debe eliminar el índice del grupo especificado.

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

```
racadm getconfig -g <nombre de grupo> -i <índice 1-16>
```

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

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
```

Si escribe `racadm getconfig -f <mi_ejemplo>.cfg`, el comando construye un archivo `.cfg` para la configuración actual del DRAC 5. Este archivo de configuración se puede usar como un ejemplo y como un punto de inicio para su archivo `.cfg` exclusivo.

Modificación de la dirección IP del DRAC 5

Cuando modifique la dirección IP del DRAC 5 en el archivo de configuración, elimine todas las anotaciones innecesarias de `<variable>=valor`. Sólo la etiqueta variable real del grupo con "[" y "]" permanecerá, incluyendo las dos anotaciones `<variable>=valor` correspondientes al cambio de la dirección IP.

Por ejemplo:

```
#  
# Object Group "cfgLanNetworking"
```

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

Este archivo se actualizará como se muestra a continuación:

```
#  
# 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. El archivo correcto será aquel que actualice las anotaciones correctas. 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 en toda la compañía o para configurar nuevos sistemas en la red.

 **NOTA:** "Ancla" es una palabra de uso interno y no se debe usar en el archivo.

Uso de la utilidad RACADM para configurar el DRAC 5

 **NOTA:** Para ejecutar los comandos de RACADM, debe iniciar sesión como usuario `root` en un sistema remoto Linux.

La interfaz basada en web del DRAC 5 es la forma más rápida de configurar un DRAC 5. Si prefiere la configuración de línea de comandos o de secuencia de comandos, o si necesita configurar varios DRAC 5, utilice RACADM, que se instala con los agentes del DRAC 5 en el sistema administrado.

Para configurar varios DRAC 5 con valores de configuración idénticos, realice uno de los siguientes procedimientos:

- 1 Use los ejemplos RACADM en esta sección como guía para crear un archivo de procesamiento en lote de comandos `racadm` y luego ejecútelo en cada sistema administrado.
- 1 Cree el archivo de configuración del DRAC 5 como se describe en "[Descripción de subcomandos de RACADM](#)" y después ejecute el subcomando `racadm config` en cada sistema administrado usando el mismo archivo de configuración.

Antes de comenzar

Puede configurar hasta 16 usuarios en la base de datos de propiedades del DRAC 5. Antes de habilitar manualmente a un usuario del DRAC 5, verifique si hay algún usuario actual. Si está configurando un DRAC 5 nuevo o si ha ejecutado el comando `racadm racresetcfg`, el único usuario actual es `root` con la contraseña `calvin`. El subcomando `racresetcfg` restablece el DRAC 5 a sus valores predeterminados originales.

 **AVISO:** Tenga precaución cuando utilice el comando `racreset.cfg`, ya que se vuelven a establecer *todos* los parámetros de configuración predeterminados originales. Se perderán todos los cambios anteriores.

 **NOTA:** Los usuarios pueden ser activados y desactivados con el transcurso del tiempo. Por consiguiente, los usuarios del DRAC 5 no tienen el mismo número de índice que el mismo usuario en otro 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 1-16:

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

 **NOTA:** También puede escribir `racadm getconfig -f <mi_archivo.cfg>` y ver o modificar 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. Dos objetos de interés son:

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

Si el objeto `cfgUserAdminUserName` no tiene un valor, el número de índice que indica el objeto `cfgUserAdminIndex` está disponible para su uso. Si aparece un nombre después del signo "=", ese índice está ocupado por ese nombre de usuario.

 **NOTA:** Cuando activa o desactiva manualmente un usuario con el subcomando `racadm config`, *debe* especificar el índice con la opción `-i`. Observe que el objeto `cfgUserAdminIndex` que se muestra en el ejemplo anterior contiene un carácter '#'. Asimismo, si usa el comando `racadm config -f racadm.cfg` para especificar cualquier número de grupos/objetos para escribirlos, el índice no se puede especificar. Un usuario nuevo se agrega al primer índice disponible. Este comportamiento permite tener más flexibilidad al configurar múltiples 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 procedimientos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los privilegios de usuario.
4. Habilite al usuario.

Ejemplo

El ejemplo a continuación describe cómo agregar un nuevo usuario de nombre "Juan" con una contraseña "123456" y privilegios de inicio de sesión en el RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -i 2 -o cfgUserPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Para verificar, use uno de los comandos siguientes:

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

Cómo quitar un usuario de DRAC 5

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

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

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

Una cadena nula de dos caracteres de comillas ("") indica al DRAC 5 que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.

Comprobación de las alertas de correo electrónico

La función 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 alertas por correo electrónico para asegurarse que el RAC pueda enviar correctamente alertas de correo electrónico a través de la red.

```
racadm testemail -i 2
```

 **NOTA:** Asegúrese que los valores de SMTP y de envíos de alertas por correo electrónico estén configurados antes de probar la función de alertas por correo electrónico. Para obtener más información, consulte "[Configuración de las alertas de correo electrónico](#)".

Cómo probar la función de alertas de capturas SNMP del RAC

La función de envío de alertas de capturas SNMP del RAC permite que las configuraciones de oyentes de capturas SNMP reciban capturas de los sucesos de sistema que se presentan en el sistema administrado.

El ejemplo a continuación muestra cómo un usuario puede probar la función de alertas de capturas SNMP del RAC.

```
racadm testtrap -i 2
```

Antes de probar la función de envío de alertas de capturas SNMP del RAC, asegúrese que los valores de SNMP y de las capturas estén configurados correctamente. Para configurar estos valores, consulte las descripciones de los subcomandos [testtrap](#) y [testemail](#).

Habilitación de un usuario del DRAC 5 con permisos

Para habilitar un usuario con permisos administrativos específicos (autoridad basada en funciones), localice primero un índice de usuario disponible realizando los pasos de "[Antes de comenzar](#)". Luego escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña:

 **NOTA:** Consulte la [tabla B-2](#) para obtener una lista de valores válidos de máscara de bits para habilitar permisos de usuario específicos. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene privilegios activados.

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

Configuración de propiedades de red del DRAC 5

Para generar una lista de las propiedades de red disponibles, escriba lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

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

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

Los comandos proporcionan la misma funcionalidad de configuración que la opción ROM en el momento del inicio cuando se le pide que teclee <Control><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 define en 0, la LAN del DRAC 5 se desactivará aun cuando DHCP esté activado.

Modos del DRAC

El DRAC 5 se puede configurar en uno de los tres modos siguientes:

- 1 Dedicado
- 1 Compartido
- 1 Compartido con protección contra fallas

La [tabla 9-3](#) proporciona una descripción de cada modo.

Tabla 9-3. Configuraciones del NIC del DRAC 5

| Modo | Descripción |
|---|--|
| Dedicado | El DRAC usa su propio NIC (de conector RJ-45) y la dirección MAC del BMC para acceder al tránsito de red. |
| Compartido | El DRAC usa el Broadcom LOM1 en el plano bidimensional. |
| Compartido con protección contra fallas | El DRAC usa Broadcom LOM1 y LOM2 en conjunto para contar con protección contra fallas. El conjunto usa la dirección MAC del BMC. |

Preguntas frecuentes

La [tabla 9-4](#) muestra una lista de preguntas frecuentes y sus respuestas.

Tabla 9-4. Uso de los comandos serie y racadm: Preguntas frecuentes

| Pregunta | Respuesta |
|---|---|
| Tras realizar un restablecimiento del DRAC 5 (con el comando <code>racadm racreset</code>), escribo un comando y aparece el mensaje siguiente: <code>racadm <nombre de comando> Transporte: ERROR: (RC=-1)</code> ¿Qué significa este mensaje? | Tiene que esperar hasta el DRAC 5 haya completado el restablecimiento antes de dar otro comando. |
| Cuando uso los comandos y subcomandos <code>racadm</code> recibo mensajes de error que no entiendo. | Al usar los comandos y subcomandos <code>racadm</code> , es posible que encuentre uno o más de los errores a continuación: <ul style="list-style-type: none">1 Mensajes de error locales: problemas como sintaxis, errores tipográficos y nombres incorrectos. Ejemplo: ERROR: <mensaje> |
| Cuando aplico el comando "ping" a 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. | Borra la tabla ARP en el sistema. |

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Glosario

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

AGP

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

ARP

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

ASCII

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

BIOS

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

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

CA

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

captura SNMP

Notificación (suceso) generada por el DRAC 5 o el BMC que contiene información sobre los cambios de estado en el sistema administrado o sobre problemas potenciales de hardware.

CD

Abreviatura de disco compacto.

CHAP

Siglas de "Challenge-Handshake Authentication Protocol" (Protocolo de autenticación de establecimiento de conexión), que es un método de autenticación usado por servidores PPP para validar la identidad del iniciador de la conexión.

CIM

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

CLI

Siglas de "command line interface" (interfaz de línea de comandos).

CLP

Siglas de "command line protocol" (protocolo de línea de comandos).

CSR

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

DDNS

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

DHCP

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

Dirección MAC

Abreviatura para dirección "media access control" (control de acceso a medios), que es una dirección única incorporada en los componentes físicos de una NIC.

disco RAM

Programa residente en la memoria que emula una unidad de disco duro. El DRAC 5 mantiene un disco RAM en su memoria.

DLL

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

DMTF

Siglas de "Distributed Management Task Force" (Grupo de trabajo de administración distribuida).

DNS

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

DRAC 5

Siglas de Dell Remote Access Controller 5.

DSU

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

Estación de administración

La estación de administración es un sistema que accede de forma remota al DRAC 5.

FQDN

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

FSMO

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

GMT

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

GPIO

Abreviatura de general purpose input/output (entrada/salida de propósito general).

GRUB

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

GUI

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

ICMB

Siglas 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

Siglas de "Internet Protocol" (Protocolo de Internet), que es un nivel de red de TCP/IP. El IP proporciona enrutamiento, fragmentación y reensamblaje de paquetes.

IPMB

Siglas de "intelligent platform management bus" (bus de administración de plataformas inteligentes), que es un bus usado en tecnología de administración de sistemas.

IPMI

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

Kbps

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

LAN

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

LDAP

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

LED

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

LOM

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

MAC

Siglas de "media access control" (control de acceso a medios), que es un subnivel de red entre un nodo de red y el nivel físico de la red.

MAP

Siglas de "Manageability Access Point" (punto de acceso de administrabilidad).

Mbps

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

MIB

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

MI

Siglas de "Medios Interfaz Independiente" (interfaz independiente de medios).

NAS

Abreviatura de network attached storage (almacenamiento conectado a red).

NIC

Siglas de "network interface card" (tarjeta de interfaz de red). Placa de circuitos de adaptador instalada en un equipo para proporcionar una conexión física a una red.

OID

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

PCI

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

POST

Siglas de "power-on self-test" (autoprueba de encendido), que es una secuencia de pruebas de diagnóstico que un sistema ejecuta automáticamente cuando se enciende.

PPP

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

RAC

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

RAM

Siglas de "random-access memory" (memoria de acceso aleatorio). La RAM es una memoria de propósito general que se puede leer y en la que se puede escribir en los sistemas y en el DRAC 5.

redirección de consola

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

registro de hardware

Registra los sucesos generados por el DRAC 5 y el BMC.

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

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

SAC

Siglas de "Special Administration Console" (consola de administración especial) de Microsoft.

SAP

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

SEL

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

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 del sistema).

SNMP

Siglas de "Simple Network Management Protocol" (Protocolo simple de administración de red), que es un protocolo diseñado para administrar nodos en una red de IP. Los DRAC 5 son dispositivos (nodos) administrados por SNMP.

SSH

Abreviatura para "Secure Shell".

SSL

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

TAP

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

TCP/IP

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

TFTP

Siglas de "Trivial File Transfer Protocol" (Protocolo trivial de transferencia de archivos, que es un protocolo de transferencia simple usado para cargar código de inicio a los dispositivos o sistemas sin discos.

UPS

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

USB

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

UTC

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

VLAN

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

VNC

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

VT-100

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

WAN

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

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Guía del usuario de Dell™ Remote Access Controller 5 con firmware versión 1.0

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

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

 **PRECAUCIÓN:** Una PRECAUCIÓN indica la posibilidad de daños a la propiedad, lesiones personales o muerte.

La información contenida en este documento puede modificarse sin previo aviso.
© 2006 Dell Inc. Todos los derechos reservados.

Queda estrictamente prohibida la reproducción de este documento en cualquier forma sin la autorización por escrito de Dell Inc.

Las marcas comerciales usadas en este texto: *Dell*, el logotipo de *DELL*, *Dell OpenManage* y *PowerEdge*, son marcas comerciales de Dell Inc.; *Microsoft* y *Windows* son marcas comerciales registradas y *Windows Server* es una marca comercial de Microsoft Corporation; *Red Hat* es una marca comercial registrada de Red Hat, Inc.; *Intel* es una marca comercial registrada de Intel Corporation; *UNIX* es una marca comercial registrada de The Open Group en los Estados Unidos y otros países.

Copyright 1998-2006 The OpenLDAP Foundation. Todos los derechos reservados. Sólo se permiten la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, según lo autoriza la licencia pública de OpenLDAP. Una copia de esta licencia está disponible en el archivo LICENSE en el directorio principal de la distribución, o bien, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Otros pueden obtener copyright de los archivos individuales y/o los paquetes contribuidos y estos pueden quedar sujetos a restricciones adicionales. Este trabajo proviene de la distribución de la versión 3.3 de LDAP de la Universidad de Michigan. La información acerca de este software está disponible en <http://www.umich.edu/~dirsvcs/ldap/>. Este trabajo también contiene materiales provenientes de fuentes públicas. Se puede obtener información adicional de OpenLDAP en <http://www.openldap.org/>. Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. Todos los derechos reservados. Sólo se permiten la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, según lo autoriza la licencia pública de OpenLDAP. Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. Todos los derechos reservados. Se permite la redistribución y el uso en las formas de código fuente y binaria, con o sin modificación, a condición de que este aviso se conserve. Los nombres de los titulares de copyright no pueden ser usados para respaldar o promover productos provenientes de este software sin el previo permiso específico por escrito. Este software se ofrece "tal cual" sin garantías explícitas ni implícitas. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. Todos los derechos reservados. Se permite la redistribución y el uso en las formas de código fuente y binaria con la condición de que este aviso se conserve y que se dé el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se puede usar para respaldar o promover productos provenientes de este software sin el previo permiso específico por escrito. Este software se ofrece "tal cual" sin garantías explícitas ni implícitas. Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc., renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc., renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Abril de 2006 Rev. A01

[Regresar a la página de contenido](#)