

Guía del usuario

[Descripción general del CMC](#)

[Instalación y configuración del CMC](#)

[Configuración del CMC para el uso de consolas de línea de comandos](#)

[Uso de la interfaz de línea de comandos de RACADM](#)

[Uso de la interfaz web del CMC](#)

[Uso de FlexAddress](#)

[Uso del CMC con Microsoft Active Directory](#)

[Administración de la alimentación](#)

[Uso del módulo iKVM](#)

[Administración de la estructura de red de E/S](#)

[Solución de problemas y recuperación](#)

[Subcomandos de RACADM](#)

[Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#)

[Uso de la interfaz del panel LCD](#)

[Glosario](#)

Notas y avisos

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

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

La información contenida en este documento puede modificarse sin previo aviso.
© 2008 Dell Inc. Todos los derechos reservados.

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

Marcas comerciales usadas en este texto: *Dell*, el logo de *DELL*, *OpenManage*, *PowerEdge* y *PowerConnect* son marcas comerciales de Dell Inc.; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT*, *Windows Server* y *Windows Vista* son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y en otros países; *Red Hat* y *Red Hat Enterprise Linux* son marcas comerciales registradas de Red Hat, Inc.; *Novell* y *SUSE* son marcas comerciales registradas de Novell Corporation en los Estados Unidos y en otros países; *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. *Avocent* es una marca comercial de Avocent Corporation; *OSCAR* es una marca comercial registrada de Avocent Corporation o de sus afiliados.

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo según lo autoriza la licencia pública de OpenLDAP. Hay una copia de esta licencia disponible en el archivo LICENSE en el directorio principal de la distribución o, como alternativa, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Hay archivos individuales y/o paquetes recibidos en contribuciones que pueden ser propiedad intelectual de terceros y están sujetos a restricciones adicionales. Este trabajo se deriva de la distribución LDAP v3.3 de la Universidad de Michigan. Este trabajo también contiene materiales que provienen de fuentes públicas. La información sobre OpenLDAP se puede obtener 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, siempre y cuando se conserve este aviso. Los nombres de los titulares de la propiedad intelectual no se deben usar para endosar o promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Se permite la redistribución y uso en formatos binario y original siempre y cuando se conserve este aviso y se conceda el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se debe usar para endosar ni promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas.

Es posible que se utilicen otros nombres y marcas comerciales en este documento para hacer referencia a las entidades que son dueñas de las marcas y nombres o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Agosto de 2008 Rev. A00

[Regresar a la página de contenido](#)

Subcomandos de RACADM

Guía del usuario

- ["?" y "? <comando>"](#)
- [arp](#)
- [chassisaction](#)
- [clrraclog](#)
- [clrsetl](#)
- [cmcchangeover](#)
- [config](#)
- [deploy](#)
- [feature](#)
- [tarieta de función](#)
- [fwupdate](#)
- [getassettag](#)
- [getchassisname](#)
- [getconfig](#)
- [getdcinfo](#)
- [getflexaddr](#)
- [getioinfo](#)
- [getkvminfo](#)
- [getled](#)
- [getmacaddress](#)
- [getmodinfo](#)
- [getniccf](#)
- [getpbinfo](#)
- [getpminfo](#)
- [getraclog](#)
- [getractime](#)
- [getredundancymode](#)
- [getsel](#)
- [getsensorinfo](#)
- [getslotname](#)
- [getssninfo](#)
- [getsvctag](#)
- [getsysinfo](#)
- [gettracelog](#)
- [help y help <comando>](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [racdump](#)
- [racreset](#)
- [racresetcfg](#)
- [serveraction](#)
- [setchassisname](#)
- [setassettag](#)
- [setflexaddr](#)
- [setled](#)
- [setniccf](#)
- [setractime](#)
- [setslotname](#)
- [setsysinfo](#)
- [sslcertdownload](#)
- [sslcertupload](#)
- [sslcertview](#)
- [sslcsrgen](#)
- [sslresetcfg](#)
- [testemail](#)
- [testtrap](#)

"?" y "? <comando>"

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

? muestra todos los subcomandos que pueden utilizarse con el comando **racadm** y ofrece una descripción en línea de cada subcomando.

? <comando> muestra la sintaxis del comando especificado.

 **NOTA:** Para obtener esta misma información también pueden utilizarse los comandos **help** y **help <comando>**.

Uso

```
racadm ?
```

```
racadm ? <comando>
```

Ejemplos

 **NOTA:** El siguiente ejemplo muestra sólo una parte del mensaje de salida para el comando **racadm ?**. Las descripciones de este ejemplo pueden diferir ligeramente de las descripciones de la sesión **racadm**.

```
1 racadm ?

help -- list racadm subcommand description
help <subcommand> -- display usage summary for a subcommand
? -- list racadm subcommand description
? <subcommand> -- display usage summary for a subcommand
arp -- display the networking arp table
```

```

chassisaction -- execute chassis or switch power-up/down/cycle or KVM powercycle
clrraclog -- clear the CMC log
clrslsel -- clear the System Event Log (SEL)
cmchangeover -- Changes the redundant state of the CMC from active to standby and vice versa
config -- modify CMC configuration properties
LEDs on a module
...
setniccfg -- modify network configuration properties
setractime -- set the time on the CMC
setslotname -- sets the name of the slot in the chassis
setsysinfo -- set the chassis name and chassis location
sslcertview -- display a CA/server certificate in the CMC
sslcsrgen -- generate a certificate CSR from the CMC
testemail -- test CMC email notifications
testtrap -- test CMC SNMP trap notifications

1 racadm ? getsysinfo

getsysinfo -- display general CMC and system information
Usage:
getsysinfo [-d] [-c] [-A]
-d : show cmc information
-c : show chassis information
-A : do not show headers or labels

```

arp

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Administrador**.

Descripción

Muestra la tabla del Protocolo de resolución de direcciones (ARP). Esta tabla almacena la asignación de números IP a direcciones MAC de las tarjetas de interfaz de red en el chasis.

Ejemplo

```

1 racadm arp

Address      HWtype HWaddress      Flags Mask  Iface
143.166.152.3 ether 00:07:84:A7:CE:BC C   eth0
143.166.152.2 ether 00:07:84:7B:9F:FC C   eth0
143.166.152.1 ether 00:00:0C:07:AC:0A C           eth0
143.166.152.113 ether 00:15:C5:48:9C:1D C eth0

```

chassisaction

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de control del chasis**.

Descripción

Ejecuta una acción de encendido en el chasis, iKVM o un servidor.

Uso

```
racadm chassisaction [-m <módulo>] <acción>
```

Opciones

[Tabla A-1](#) describe las opciones del subcomando **chassisaction**.

Tabla A-1. Opciones del subcomando chassisaction

Opción	Descripción
-m <módulo>	Especifica el módulo en el que debe ejecutarse la acción. El <módulo> puede estar representado por una de las siguientes opciones:

	<ul style="list-style-type: none"> chassis switch-<i>n</i> donde <i>n</i>=1-6 kvm
<acción>	<p>Especifica la acción que se desea ejecutar en el módulo indicado. La <acción> puede estar representada por una de las siguientes opciones:</p> <ul style="list-style-type: none"> powerdown: (sólo para el chasis) apaga el chasis. powerup: (sólo para el chasis) enciende el chasis. powercycle: ejecuta el ciclo de encendido del módulo. nongraceshutdown: (sólo para el chasis) apaga el chasis de manera no ordenada. reset: lleva a cabo un restablecimiento forzado del módulo.

Ejemplo

```
| racadm chassisaction -m switch-3 reset

Module power operation successful. (La operación de encendido del módulo se realizó correctamente.)
```

clrraclog

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Administrador de borrado de registros**.

Descripción

Elimina todas las entradas existentes del registro de CMC. Para registrar la fecha y la hora en que se borró el registro se agrega una nueva entrada con el nombre del usuario que realizó la operación.

 **NOTA:** Para ver el registro del CMC, utilice [getraclog](#). Para obtener información sobre el registro del CMC, consulte [Cómo ver el registro del CMC](#).

Uso

```
racadm clrraclog
```

 **NOTA:** La opción -A se ignora y se admite para proporcionar compatibilidad hacia atrás para secuencias existentes.

Salida

El registro de CMC se borró correctamente.

clrssel

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Administrador de borrado de registros**.

Descripción

Elimina todas las entradas existentes del registro de sucesos del sistema (SEL o registro de hardware). Para registrar la fecha y la hora en que se borró el registro se agrega una nueva entrada con el nombre del usuario que realizó la operación.

 **NOTA:** Para acceder al registro de hardware, utilice el comando [getssel](#). Para obtener información sobre el registro de hardware, consulte [Cómo ver el registro de hardware](#).

Uso

```
racadm clrssel
```

 **NOTA:** Las opciones -A y -o no generan mensajes de salida adicionales y se admiten para proporcionar compatibilidad hacia atrás para secuencias existentes.

Salida

```
The SEL was cleared successfully.
```

(El registro SEL se borró correctamente.)

cmchangeover

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Cambia el estado de CMC de activo a espera o viceversa, en una configuración de CMC redundante. Este subcomando es útil para la depuración remota de errores o para fines de prueba.

 **NOTA:** Este comando sólo es válido en entornos de CMC redundantes. Para obtener más información, consulte [Comprensión del entorno de CMC redundante](#).

Uso

```
racadm cmchangeover
```

Salida

```
CMC failover initiated successfully.
```

(La protección contra fallas de CMC se inició correctamente.)

config

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Define los parámetros de configuración de CMC por separado o en un lote como parte de un archivo de configuración. Si los datos difieren, el objeto CMC se escribe con los nuevos valores.

Uso

```
racadm config -g <grupo> -o <objeto> <valor>
```

```
racadm config -g <grupo> -o <objeto> -i <indice> <valor>
```

```
racadm config -f <nombre_de_archivo>
```

Opciones

[Tabla A-2](#) describe las opciones del subcomando **config**.

Tabla A-2. Opciones del subcomando **config**

Opción	Descripción
-g <grupo>	Especifica el grupo que contiene el objeto a definir. Debe utilizarse con la opción -o. Tabla A-3 enumera los nombres de grupo que pueden especificarse con esta opción.
-o <objeto>	Especifica el nombre del objeto escrito con la cadena de caracteres <valor>. Debe utilizarse con la opción -g.
-i <indice>	Especifica un nombre exclusivo de grupo. Sólo es válido para los grupos indexados. En este caso el índice es especificado por el valor de índice (un número decimal entre 1 y 16).
<valor>	Indica el valor que se utilizará para definir el objeto especificado.
-f <nombre de archivo>	Indica el nombre del archivo que se utilizará como archivo de origen de la configuración.

Grupos de propiedades

 **NOTA:** Apéndice B, [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#), proporciona detalles sobre los grupos de propiedades. Consulte también [getconfig](#).

[Tabla A-3](#) muestra una lista de los grupos de propiedades que pueden especificarse con la opción -g.

Tabla A-3. Grupos de propiedades de RACADM

Grupo	Descripción
cfgLanNetworking	Configura las propiedades relacionadas con la red
cfgRemoteHosts	Activa o desactiva y configura las actualizaciones de firmware y las alertas por correo electrónico de SMTP
cfgUserAdmin	Configura los usuarios del CMC
cfgEmailAlert	Configura las alertas por correo electrónico de SMTP
cfgSessionManagement	Define la cantidad máxima de sesiones remotas permitidas para conectarse al CMC de forma simultánea
cfgSerial	Activa o desactiva y configura la consola serie
cfgNetTuning	Configura los ajustes de red del CMC
cfgOobSnmp	Activa o desactiva y configura las capturas SNMP del CMC
cfgTraps	Muestra información y configura el envío de capturas SNMP para un usuario determinado
cfgAlerting	Activa o desactiva las alertas de captura de sucesos de SNMP y define el filtro de sucesos
cfgRacTuning	Configura los parámetros de ajustes del CMC
cfgRacSecurity	Define los valores de configuración relacionados con la función de solicitud de firma de certificado (CSR) SSL del CMC
cfgActiveDirectory	Configura las propiedades de Microsoft® Active Directory®
cfgStandardSchema	Define la configuración del esquema estándar de Active Directory
cfgChassisPower	Configura la alimentación del chasis
cfgServerInfo	Configura un servidor en el chasis
cfgKVMInfo	Muestra información y configura el iKVM

Salida

El subcomando **config** genera un mensaje de error al detectar alguno de los siguientes factores:

- 1 Sintaxis, nombre de grupo, nombre de objeto o índice no válidos, u otros miembros no válidos de la base de datos
- 1 Privilegios de usuario insuficientes
- 1 Fallas de la CLI de RACADM
- 1 El subcomando **config** indica la cantidad de objetos de configuración escritos en comparación con el total de objetos incluidos en el archivo **.cfg**.

Ejemplos

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

Define el parámetro de configuración (objeto) **cfgNicIpAddress** con el valor 10.35.10.110. Este objeto de dirección IP está incluido en el grupo **cfgLanNetworking** (consulte [cfgLanNetworking](#)).

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

Configura o vuelve a configurar el CMC. El usuario puede crear el archivo **myrac.cfg** por medio del comando **getconfig**. También es posible editar de forma manual el archivo **myrac.cfg**, siempre y cuando se sigan las reglas de análisis (consulte [Reglas del análisis](#)).

 **NOTA:** El archivo **myrac.cfg** no contiene información de contraseña. Para incluir información de contraseñas en este archivo es necesario ingresarla manualmente.

deploy

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Server Administrator**.

Descripción

Configura la dirección IP estática, máscara de subred, puerta de enlace y contraseña del usuario "root" del iDRAC para el servidor especificado.

 **NOTA:** Este subcomando sólo es válido si la opción DHCP está desactivada para el servidor que se especifica. Si la opción DHCP está activada, el servidor obtiene automáticamente la dirección IP, máscara de subred y puerta de enlace del servidor DHCP. Para determinar si esta opción se encuentra activada para el servidor, utilice el comando **getniccfg** (consulte [getniccfg](#)). Para activar o desactivar DHCP, utilice el comando **setniccfg** (consulte [setniccfg](#)).

 **NOTA:** También es posible utilizar el comando `setniccfg` para configurar la dirección IP estática, máscara de subred y puerta de enlace, además de las propiedades de DHCP, velocidad y dúplex. Para obtener más información, consulte [setniccfg](#).

Uso

```
racadm deploy -m <módulo> -u root -p <contraseña>
[-s <dirección ip> <subred> <puerta de enlace>] [-d]
```

Opciones

[Tabla A-4](#) describe las opciones del subcomando `deploy`.

Tabla A-4. Opciones del subcomando `deploy`

Opción	Descripción
-u root	Indica que la <contraseña> será determinada por el usuario root en el servidor. root es un parámetro constante, el único valor válido con la opción -u.
-m <módulo>	Especifica el servidor que se desea configurar. Valores legales: servidor- <i>n</i> , donde <i>n</i> =1-16
-p <contraseña>	Especifica la contraseña del usuario "root" en el servidor.
-s <dirección_ip subred puerta_de_enlace>	Define la dirección IP, la máscara de subred y la puerta de enlace del servidor especificado, separados por un espacio. 1 dirección_IP: cadena de caracteres que representa una dirección IP válida. Por ejemplo, 192.168.0.20. 1 subred: cadena de caracteres que representa una máscara de subred válida. Por ejemplo: 255.255.255.0. 1 puerta_de_enlace: cadena de caracteres que representa una máscara de subred válida. Por ejemplo, 192.168.0.1.
-d	Activa DHCP para el usuario especificado.

Ejemplo

```
1 racadm deploy server-8 -s 192.168.0.20 255.255.255.0 192.168.0.1
```

The server was deployed successfully.

(El servidor se implementó correctamente.)

 **NOTA:** El comando `deploy` genera un error cuando se lo utiliza en la ranura de extensión de un servidor con múltiples ranuras.

```
1 racadm deploy -m server-9 192.168.0.11 255.255.255.0 192.168.0.1
```

ERROR: Server in slot 9 is an extension of the server in slot 1.

(ERROR: el servidor en la ranura 9 es una extensión del servidor en la ranura 1.)

feature

 **NOTA:** Para utilizar este subcomando para desactivar FlexAddress, debe contar con privilegios de **Administrador de configuración del chasis**. Un usuario con privilegios de inicio de sesión sólo puede ver el estado.

Descripción

Muestra todas funciones activados en el chasis. La información que se muestra incluye el nombre de la función, la fecha de activación y el número de serie de la tarjeta SD usada para activar la función.

 **NOTA:** El subcomando `feature` debe ejecutarse cuando el chasis esté apagado para desactivar FlexAddress o el comando mostrará un error.

Uso

```
racadm feature [-s] [-d -c <nombre de función>]
```

<nombre de función> = FlexAddress

Opciones

[Tabla A-5](#) describe las opciones del subcomando **feature**.

Tabla A-5. Opciones del subcomando feature

Opción	Descripción
-d -c <nombre de función>	Desactiva la función.
-s	Muestra las funciones activadas.

Ejemplo

```
l racadm feature -d -c flexaddress

feature FlexAddress is deactivated on the chassis successfully

(la función FlexAddress se ha desactivado en el chasis satisfactoriamente.)

l racadm feature -s

Feature = FlexAddress

Date Activated = 8 April 2008 - 10:39:40

Feature installed from SD card SN = 01122334455

(Función = FlexAddress

Fecha de activación = 8 de abril de 2008 - 10:39:40

Función instalada desde la tarjeta SD SN = 01122334455)
```

tarjeta de función

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Verifica la correcta instalación de la tarjeta SD y muestra el estado de la misma. La siguiente tabla muestra los mensajes de estado que muestra el comando.

Tabla A-6. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
No se insertó ninguna tarjeta de función.	Controle el CMC para verificar que la tarjeta SD se haya insertado correctamente. En una configuración de CMC redundante, asegúrese de que el CMC con la tarjeta de función SD instalada sea el CMC activo y no el CMC en espera.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está sujeta a este chasis	No es necesaria ninguna acción.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está sujeta a otro chasis, svctag = ABC1234, tarjeta SD SN = 01122334455	Retire la tarjeta SD; coloque e instale la tarjeta SD para el chasis actual.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función no está sujeta a ningún chasis	La tarjeta de función se puede mover a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, ingrese <i>racadm racreset</i> hasta que se active el módulo del CMC con la tarjeta de función instalada.

Uso

```
racadm featurecard -s
```

Opciones

[Tabla A-7](#) describe las opciones del subcomando `featurecard`.

Tabla A-7. Opciones del subcomando `featurecard`

Opción	Descripción
-s	Muestra las funciones activadas de la tarjeta SD y el estado de la misma.

Ejemplo

```
racadm featurecard -s
```

```
1 racadm featurecard -s
```

```
The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis
```

```
(La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está sujeta a este chassis)
```

fwupdate

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Actualiza el firmware en el iKVM, el CMC principal, el CMC en espera (si corresponde), el iDRAC del servidor y el dispositivo de infraestructura del módulo de E/S. Asimismo, realiza actualizaciones del firmware del iDRAC si está dañado.

 **NOTA:** Si ejecuta el subcomando `fwupdate` para actualizar el firmware del CMC principal, todas las conexiones Telnet y web quedarán interrumpidas. Para supervisar el progreso del proceso de actualización, utilice la opción `-s`. Durante la actualización de todos los módulos restantes, incluso el CMC en espera, el CMC principal continuará ejecutándose normalmente sin necesidad de restablecer el sistema.

 **NOTA:** El subcomando `fwupdate` sólo puede ejecutarse en un dispositivo a la vez en el iKVM. En los CMC, los servidores y los dispositivos de infraestructura del módulo de E/S se pueden actualizar varios dispositivos a la vez.

Uso

```
racadm fwupdate -g -u -a <dirección ip del servidor tftp> [-f <dirección ip del servidor ftp> <nombre de usuario> <contraseña>] -d <ruta de acceso> -m <destino>
```

```
racadm fwupdate -s
```

```
racadm fwupdate -c
```

Opciones

En la [tabla A-8](#) se describen las opciones del subcomando `fwupdate`.

Tabla A-8. Opciones del subcomando `fwupdate`

Opción	Descripción
-d <ruta de acceso>	Especifica la ruta de acceso de origen en la que reside la imagen del firmware. Predefinido: directorio local en CMC si la opción <code>-g</code> está ausente. Si se usa <code>-g</code> , se predetermina al directorio configurado en el servidor TFTP.
-g	Descarga la actualización de firmware por medio del servidor TFTP.
-u	Ejecuta la actualización del firmware (se utiliza con <code>-g</code>).
-a <dirección ip del servidor tftp>	Especifica la dirección IP del servidor TFTP que se usa para la imagen del firmware (se utiliza con <code>-g</code>).
-f <dirección ip del servidor ftp> <nombre de usuario> <contraseña>	Especifica la dirección IP del servidor FTP que se utiliza para la imagen del firmware, junto con el nombre de usuario y la contraseña. Sólo puede usarse con dispositivos de destino de CMC, iKVM y del servidor iDRAC.
-m <destino>	Especifica el destino, o el dispositivo, que se actualizará. <destino> está representado por uno de los siguientes valores:

	<pre> 1 cmc-active (predeterminado) 1 cmc-standby 1 kvm 1 server-n donde n = 1-16 1 iomifn-n donde n = 1-6 </pre> <p>NOTA: Los destinos <code>cmc-active</code> y <code>cmc-standby</code> pueden escribirse juntos, así como uno o más <code>server-n</code>, y uno o más destinos <code>iomifn-n</code> para que los dispositivos se puedan actualizar juntos.</p>
<code>-s</code>	Muestra el estado actual de la actualización de firmware.
<code>-c</code>	Cancela la actualización de firmware actual.

 **NOTA:** Antes de verificar el estado de la actualización, aguarde hasta que finalice la transferencia del archivo desde el servidor TFTP.

 **NOTA:** Cuando usa FTP, si la ruta de acceso completa al archivo de imagen se proporciona en la CLI, se usará esa ruta de acceso para ubicar el archivo en el host. Si no se proporciona la ruta de acceso, se busca el directorio principal del usuario especificado para el archivo si el sistema central ejecuta Linux o alguna otra variante de UNIX. Si el sistema central ejecuta Windows, se busca la carpeta predeterminada (como **ftproot**).

Ejemplo

```

1 racadm fwupdate -g -u -a 192.168.0.120 -d firmimg.cmc -m cmc-active

TFTP firmware update has been initiated. This update process may take several minutes to complete.

Firmware update complete.

(Se ha iniciado la actualización del firmware del TFTP. Esta actualización puede tardar varios minutos en completarse.

Actualización de firmware completa.)

1 racadm fwupdate -s -m cmc-active

Firmware update in progress.

(Actualización de firmware en progreso.)

```

 **NOTA:** El comando `fwupdate` genera un error cuando se lo utiliza en la ranura de extensión de un servidor con múltiples ranuras.

```

1 racadm fwupdate -g -u -a 192.168.0.120 -d update -m server-9

ERROR: Server in slot 9 is an extension of the server in slot 1.

(ERROR: el servidor en la ranura 9 es una extensión del servidor en la ranura 1.)

```

getassettag

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra la etiqueta de propiedad del chasis.

Uso

```
racadm getassettag [-m <módulo>]
```

Opciones

[Tabla A-9](#) describe las opciones del subcomando `getassettag`.

Tabla A-9. Opciones del subcomando `getassettag`

Opción	Descripción
<code>-m <módulo></code>	<p>Especifica el módulo cuya etiqueta de propiedad se desea visualizar.</p> <p>Valor legal: chasis</p>

Dado que existe un único valor legal, puede obtenerse la misma información aun sin incluir esta opción.

Ejemplo

```
l racadm getassettag -m chassis
```

O bien:

```
racadm getassettag  
chassis 78373839-33
```

getchassisname

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el nombre del chasis.

Uso

```
racadm getchassisname
```

Ejemplo

```
l racadm getchassisname  
PowerEdge 2955
```

getconfig

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Muestra los parámetros de configuración del CMC y permite guardar los grupos de configuraciones en un archivo .cfg.

Uso

```
racadm getconfig -g <nombre de grupo>  
racadm getconfig -g <nombre de grupo> -o <objeto>  
racadm getconfig -g <nombre de grupo> -i <indice>  
racadm getconfig -u <nombre_de_usuario>  
racadm getconfig -h  
racadm getconfig -f <nombre de archivo>
```

Opciones

[Tabla A-10](#) describe las opciones del subcomando `getconfig`.

Tabla A-10. Opciones del subcomando getconfig

Opción	Descripción
--------	-------------

-g <nombre_de_grupo>	Especifica el grupo que contiene el objeto a definir. Debe utilizarse con la opción -o. Tabla A-11 muestra los grupos que puede especificar.
-o <nombre_de_objeto>	Especifica el nombre del objeto escrito con la cadena de caracteres <valor>. Debe utilizarse con la opción -g.
-i <índice>	Especifica un nombre exclusivo de grupo. Sólo es válido para los grupos indexados. El índice es determinado por el valor de índice (un número decimal entre 1 y 16).
-u	Muestra el grupo vinculado con un usuario determinado.
-h	Muestra una lista de los grupos de configuración disponibles.
-f <nombre_de_archivo>	Guarda la configuración del CMC en un archivo .cfg, a través del nombre de archivo especificado.

Grupos de propiedades

 **NOTA:** [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#), proporciona detalles sobre estos grupos de propiedades. Consulte también [config](#).

[Tabla A-11](#) muestra una lista de los grupos de propiedades que pueden especificarse con la opción -g del subcomando `getconfig`.

Tabla A-11. Grupos de propiedades del subcomando `getconfig`

Grupo de propiedades	Descripción
idRacInfo (sólo lectura)	Muestra la versión, el número de modelo e información de producto del CMC.
cfgLanNetworking	Configura las propiedades relacionadas con la red.
cfgCurrentLanNetworking (sólo lectura)	Muestra las propiedades actuales de la tarjeta de interfaz de red del CMC.
cfgRemoteHosts	Activa o desactiva y configura las actualizaciones de firmware y alertas por correo electrónico de SMTP.
cfgUserAdmin	Configura los usuarios del CMC.
cfgEmailAlert	Configura las alertas por correo electrónico de SMTP.
cfgSessionManagement	Define la cantidad máxima de sesiones remotas permitidas para conectarse al CMC de forma simultánea.
cfgSerial	Activa o desactiva y configura la consola serie.
cfgNetTuning	Configura los ajustes de red del CMC.
cfgObSnmp	Activa o desactiva y configura las capturas SNMP del CMC.
cfgTraps	Configura el envío de capturas SNMP para un usuario determinado.
cfgAlerting	Activa o desactiva las alertas de captura de sucesos de SNMP y define el filtro de sucesos.
cfgRacTuning	Configura los parámetros de ajustes del CMC.
cfgRacSecurity	Define la configuración relacionada con la solicitud de firma de certificado (CSR) SSL del CMC.
cfgActiveDirectory	Configura las propiedades de Microsoft Active Directory.
cfgStandardSchema	Define la configuración del esquema estándar de Active Directory.
cfgChassisPower	Configura la alimentación del chasis
cfgServerInfo	Configura un servidor en el chasis
cfgKVMInfo	Muestra información y configura el iKVM

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 no válidos, u otros miembros no válidos 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) incluidas en el grupo `cfgLanNetworking` (consulte [cfgLanNetworking](#)).

```
1 racadm getconfig -g cfgserverinfo -o cfgservername 123456789012345
```

Guarda el nombre de ranura del servidor; el nombre de ranura puede tener como máximo 15 caracteres (consulte [cfgServerName](#)).

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

Guarda todos los objetos de configuración del grupo del CMC en myrac.cfg.

```
1 racadm getconfig -h
```

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

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

Muestra las propiedades de configuración del usuario root.

getdcinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información general sobre el módulo de E/S y la configuración de la tarjeta subordinada.

 **NOTA:** La verificación de la estructura de red de DC del servidor sólo se realiza cuando el chasis está encendido. Si el chasis está en espera, los iDRAC de los módulos del servidor permanecen apagados y por tanto no pueden brindar información sobre el tipo de estructura de red de DC del servidor. El tipo de estructura de red de DC no aparecerá en la interfaz de usuario del CMC hasta que el iDRAC del servidor se encienda.

Uso

```
racadm getdcinfo
```

 **NOTA:** El siguiente ejemplo de mensaje de salida se aplica a un sistema con ranuras múltiples.

Ejemplo

```
1 racadm getdcinfo

Group 1 I/O Type : Gigabit Ethernet
Group 2 I/O Type : FibreChannel 8
Group 3 I/O Type : Infiniband DDR

<N° de E/S>          <Tipo>                <Estado>
switch-1            Gigabit Ethernet      OK
switch-2            Gigabit Ethernet      OK
switch-3            FibreChannel 8        OK
switch-4            FibreChannel 8        OK
switch-5            Infiniband DDR        OK
switch-6            Infiniband DDR        OK

<N° servidor> <Presencia> <Tipo de DC1> <Estado de DC1>
<Tipo de DC2> <Estado de DC2>

server-1 Present FibreChannel 8 OK
Infiniband DDR OK
server-2 Not Present None N/A
None N/A
server-3 Present FibreChannel 8 OK
Infiniband DDR OK
server-4 Not Present None N/A
None N/A
server-5 Not Present None N/A
None N/A
server-6 Not Present None N/A
None N/A
server-7 Not Present None N/A
None N/A
server-8 Not Present None N/A
None N/A
server-9 Extension(1) FibreChannel 8 OK
Infiniband DDR OK
server-10 Not Present None N/A
None N/A
server-11 Not Present None N/A
None N/A
server-12 Not Present None N/A
None N/A
server-13 Not Present None N/A
None N/A
server-14 Not Present None N/A
None N/A
server-15 Not Present None N/A
None N/A
server-16 Not Present None N/A
```

getflexaddr

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el estado activado/desactivado para todo el chasis. Si se utiliza con `-i`, el comando muestra las MAC/WWN por ranura.

 **NOTA:** Si FlexAddress no está activado en el chasis, el comando muestra las direcciones MAC/WWN asignadas por el servidor. Si la ranura está vacía, el comando mostrará un mensaje de error.

Uso

```
racadm getflexaddr [-i <N° ranura>]
```

<N° ranura> = 1 a 16

Opciones

[Tabla A-12](#) describe las opciones del subcomando `getflexaddr`.

Tabla A-12. Opciones del subcomando getflexaddr

Opción	Descripción
<code>-i</code>	Especifica la información de la ranura que se mostrará.

Ejemplo

```
1 racadm getflexaddr
   <N° ranura> <Nombre de ranura> <Estado>
1 slot-1 enabled
2 slot-2 enabled
3 slot-3 disabled
4 slot-4 disabled
5 slot-5 disabled
6 slot-6 disabled
7 slot-7 disabled
8 slot-8 disabled
9 slot-9 disabled
10 slot-10 disabled
11 slot-11 disabled
12 slot-12 disabled
13 slot-13 disabled
14 slot-14 disabled
15 slot-15 disabled
16 slot-16 disabled
<Estructura de red> <Tipo> <Estado>
```

```
Fabric-A ethernet disabled

Fabric-B iSCSI enabled

Fabric-C fiber channel enabled

1 racadm getflexaddr -i 1

Ranura-1 flexaddress activada = 1

<Estructura de red> <Tipo> <Asignada por el servidor>
<Asignada por el chasis>

slot1-A1 Gigabit Ethernet 00:1C:23:CD:AC:D2(active)
00:1E:C9:FF:E3:21
iSCSI 00:1C:23:CD:AC:D3(active)
00:1E:C9:FF:E3:22
slot1-A2 Gigabit Ethernet 00:1C:23:CD:AC:D4(active)
00:1E:C9:FF:E3:23
iSCSI 00:1C:23:CD:AC:D5(active)
00:1E:C9:FF:E3:24
slot1-B1 Gigabit Ethernet 00:1D:09:71:B3:60
00:1E:C9:FF:E3:25(active)
iSCSI 00:1D:09:71:B3:61
00:1E:C9:FF:E3:26(active)
slot1-B2 Gigabit Ethernet 00:1D:09:71:B3:62
00:1E:C9:FF:E3:27(active)
iSCSI 00:1D:09:71:B3:63
00:1E:C9:FF:E3:28(active)
slot1-C1 Fiber Channel 4 10:00:00:00:C9:63:51:0E
20:01:00:1E:C9:FF:E3:29(active)
slot1-C2 Fiber Channel 4 10:00:00:00:C9:63:51:0D
20:02:00:1E:C9:FF:E3:29(active)
```

getioinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información general sobre los módulos de E/S del chasis.

 **NOTA:** El tipo de estructura de red puede ser cualquier de cualquier tipo de estructura de red de E/S admitido, como Ethernet, Fiber Channel o Infiniband.

Uso

```
racadm getioinfo
```

Ejemplo

```
racadm getioinfo

<E/S> <Nombre> <Tipo> <presencia> <POST> <Alimentación>
switch-1 Ethernet Passthrough Gigabit Ethernet Present

OK ON
switch-2 N/A None Not Present

N/A N/A
switch-3 N/A None Not Present

N/A N/A
switch-4 N/A None Not Present

N/A N/A
switch-5 N/A None Not Present

N/A N/A
switch-6 N/A None Not Present

N/A N/A
```

getkvminfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información sobre el módulo iKVM.

Uso

```
racadm getkvminfo
```

Ejemplo

```
racadm getkvminfo  
  
<módulo> <presencia> <modelo> <Versión de FW> <estado>  
KVM Present Avocent iKVM Switch 00.05.00.04 Ready
```

getled

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra la configuración del indicador LED de un módulo: parpadeando, sin parpadear o desconocido (para las ranuras vacías).

Uso

```
racadm getled -m <módulo>
```

[Tabla A-13](#) describe las opciones del subcomando **getled**.

Tabla A-13. Opciones del subcomando getled

Opción	Descripción
-m <módulo>	Especifica el módulo cuya configuración de LED se desea conocer. El <módulo> puede ser una de las siguientes opciones: <ul style="list-style-type: none"> server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6 chassis cmc-active

Ejemplos

```
| racadm getled -m server-10  
  
<módulo> <estado>  
server-10 Blinking (Parpadeando)  
  
| racadm getled -m chassis  
  
<módulo> <estado>  
server-10 Not blinking (Sin parpadear)  
  
| racadm getled -m server-1  
  
<módulo> <estado>  
server-1 ON (Encendido)  
  
racadm getled -m server-9
```

<módulo> <estado>
server-9 Extensión(1)

getmacaddress

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra las direcciones MAC/WWN de todos los módulos o un módulo especificado.

Uso

```
racadm getmacaddress [-m <módulo>] [<-t iscsi>]
```

```
racadm getmacaddress [-a]
```

Opciones

[Tabla A-14](#) describe las opciones del subcomando **getmacaddress**.

Tabla A-14. Opciones del subcomando **getmacaddress**

Opción	Descripción
-m <módulo>	Especifica el módulo cuya dirección MAC se desea conocer. El <módulo> puede estar representado por una de las siguientes opciones: <ul style="list-style-type: none"> chasis server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6
-t	Muestra las direcciones MAC de iSCSI para todos los servidores o para el servidor especificado si se usa con la opción -m.
-a	Muestra las direcciones MAC/WWN de iSCSI y Ethernet para todos los iDRAC/LOM/tarjetas intermedias. Cuando se activa FlexAddress para una ranura particular, se muestra la dirección MAC/WWN asignada por el chasis.

Ejemplo

```
racadm getmacaddress -m server-1
```

```
<Nombre> <Presencia> <Dirección MAC de BMC> <Dirección MAC de NIC1> <Dirección MAC de NIC2>  
server-1 Present 00:11:43:FD:B7:2A 00:11:43:FD:B7:2A 00:11:43:FD:B7:2B  
server-9 Extension(1) N/A 00:11:43:FD:B7:2C 00:11:43:FD:B7:2D
```

getmodinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

En los módulos que no cuentan con etiquetas de servicio este campo estará en blanco.

Descripción

Muestra información sobre la configuración y el estado de todos los módulos o un módulo determinado (servidor, conmutador, CMC, unidad de ventilador o de suministro de energía) del chasis.

Uso

```
racadm getmodinfo [-m <módulo>] [-A]
```

Opciones

Tabla A-15 describe las opciones del subcomando `getmodinfo`.

Tabla A-15. Opciones de subcomando `getmodinfo`

Opción	Descripción
-m <módulo>	Especifica el módulo cuya configuración y estado se desean conocer. El comando predeterminado (sin opciones) muestra información sobre todos los componentes principales del chasis. El <módulo> puede estar representado por cualquiera de los siguientes valores: <ul style="list-style-type: none"> server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6 CMC-<i>n</i> donde <i>n</i>=1 (principal), 2 (en espera) fan-<i>n</i> donde <i>n</i>=1-9 ps-<i>n</i> donde <i>n</i>=1-6 kvm chassis
-A	Suprime los encabezados y las etiquetas al brindar la información.

Ejemplo

```
l racadm getmodinfo -m switch-1

<módulo>      <presencia>   <estado de alimentación>  <estado>      <etiqueta de servicio>
Switch-1 Present ON OK ABC1234

l racadm getmodinfo

<módulo>      <presencia>   <estado de alimentación>  <estado>      <etiqueta de servicio>
Chassis Present ON Not OK ABC1234
Fan-1 Present ON OK
Fan-2 Present ON OK
Fan-3 Present ON OK
Fan-4 Present ON OK
Fan-5 Present ON OK
Fan-6 Present ON OK
Fan-7 Present ON OK
Fan-8 Present ON OK
Fan-9 Present ON OK
PS-1 Present Online OK
PS-2 Not Present N/A N/A N/A
PS-3 Present Online OK
PS-4 Not Present N/A N/A N/A
PS-5 Not Present N/A N/A N/A
PS-6 Not Present N/A N/A N/A
CMC-1 Present Primary OK N/A
CMC-2 Not Present N/A N/A N/A
Switch-1 Not Present N/A N/A N/A
Switch-2 Not Present N/A N/A N/A
Switch-3 Not Present N/A N/A N/A
Switch-4 Not Present N/A N/A N/A
Switch-5 Not Present N/A N/A N/A
Switch-6 Not Present N/A N/A N/A
Server-1 Not Present N/A N/A N/A
Server-2 Present OFF OK
Server-3 Present ON OK S YW
Server-4 Present ON OK
Server-5 Present ON OK
Server-6 Present ON OK 1234567
Server-7 Present ON OK
Server-8 Not Present N/A N/A N/A
Server-9 Not Present N/A N/A N/A
Server-10 Extension(2) N/A N/A N/A
Server-11 Not Present N/A N/A N/A
Server-12 Present ON OK
Server-13 Not Present N/A N/A N/A
Server-14 Present ON OK 0000015 Server-15 Present ON OK
Server-16 Present ON OK
KVM Present ON OK
```

getniccfg

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra la configuración de red de un servidor, conmutador o el chasis.

 **NOTA:** Si la operación no es satisfactoria, el subcomando `getniccfg` muestra el mensaje de error.

Uso

```
racadm getniccfg [-m <módulo>]
```

Opciones

[Tabla A-16](#) describe las opciones del subcomando `getniccfg`.

Tabla A-16. Opciones del subcomando getniccfg

Opción	Descripción
-m <módulo>	<p>Especifica el módulo cuya configuración de red se desea conocer.</p> <p>El <módulo> puede ser cualquiera de las siguientes opciones:</p> <ul style="list-style-type: none"> chasis server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6 <p>Valor predeterminado: chasis</p>

Ejemplos

```
racadm getniccfg

NIC Enabled = 1
DHCP Enabled = 1
Static IP Address = 192.168.0.120
Static Subnet Mask = 255.255.255.0
PStatic Gateway = 192.168.0.1
Current IP Address = 10.35.155.160
Current Subnet Mask = 255.255.255.0
Current Gateway = 10.35.155.1
Speed = Autonegotiate
Duplex = Autonegotiate

| racadm getniccfg -m server-1

DHCP Enabled = 0
IP Address = 192.168.0.135
Subnet Mask = 255.255.255.0
Gateway = 192.168.0.1

| racadm getniccfg -m server-9

ERROR: Server in slot 9 is an extension of the server in slot 1.
```

getpbinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información del estado del presupuesto de alimentación.

Uso

```
racadm getpbinfo
```

Ejemplo

```
racadm getpbinfo
```

```
[Estado del presupuesto de alimentación]
System Input Power = 700 W
Peak System Power = 0 W
Peak System Power Timestamp = 01:08:23 01/27/2009
Minimum System Power = 0 W
Minimum System Power Timestamp = 20:18:30 01/27/2000
Overall Power Health = Not OK
Redundancy = No
System Input Power Cap = 7928 W
Redundancy Policy = None
Dynamic PSU Engagement Enabled = No
System Input Max Power Capacity = 0 W
Input Redundancy Reserve = 0 W
Input Power Allocated to Servers = 0 W
Input Power Allocated to Chassis Infrastructure = 51 watts
Total Input Power Available for Allocation = 0 W
Standby Input Power Capacity = 0 W

[Tabla de estado de suministro de energía del chasis]
<Nombre> <Presencia> <Estado de alimentación> <Corriente de entrada> <Voltios de entrada> <Calificación de salida>
PS1 Online On 16.1 A 32 V

2360 W
PS2 Not Present Slot Empty N/A N/A

N/A
PS3 Not Present Slot Empty N/A N/A

N/A
PS4 Not Present Slot Empty N/A N/A

N/A

PS5 Not Present Slot Empty N/A N/A

N/A

PS6 Not Present Slot Empty N/A N/A

N/A

[Tabla asignación de alimentación al módulo del servidor]
<Nº ranura><Nombre del servidor><Estado de alimentación><Asignación><Prioridad><Tipo de cuchilla>

1 SLOT-01 N/A N/A 5 N/A
2 SLOT-02 OFF 0 W 5 PowerEdgeM805
3 SLOT-03 ON 164 W 5 N/A
4 SLOT-04 ON 155 W 5
5 SLOT-05 ON 180 W 5
6 SLOT-06 ON 180 W 5 PowerEdgeM600
7 SLOT-07 ON 170 W 5
8 SLOT-08 N/A N/A 5 N/A
9 SLOT-09 N/A N/A 5 N/A
10 SLOT-10 Extension(2) N/A 5 N/A
11 SLOT-11 N/A N/A 5 N/A
12 SLOT-12 ON 125 W 5 PowerEdgeM600
13 SLOT-13 N/A N/A 5 N/A
14 SLOT-14 ON 342 W 5 N/A
15 SLOT-15 ON 140 W 5
16 SLOT-16 ON 125 W 5 N/A
```

getpminfo

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información del estado de administración de alimentación.

Uso

```
racadm getpminfo
```

Ejemplo

```
racadm getpminfo
```

```
[Estadísticas de alimentación de tiempo real]
System Input Power = 600 W (188 BTU/hr)
Peak System Power = 600 W (188 BTU/hr)
Peak System Power Start Time = 16:02:10 01/16/2008
Peak System Power Timestamp = 06:32:55 01/26/2009
Minimum System Power = 400 W (177 BTU/hr)
Minimum System Power Start Time = 22:43:21 01/21/2008
Minimum System Power Timestamp = 06:32:55 01/26/2009
System Idle Power = 68 W (188 BTU/hr)
System Potential Power = 68 W (188 BTU/hr)
System Input Current Reading = 31.2 A

[Estadísticas de energía de tiempo real]
System Energy Consumption = 6.4 kWh
System Energy Consumption Start Time = 16:02:10 01/16/2008
System Energy Consumption Timestamp = 16:02:10 01/16/2008

[Estado de la alimentación del sistema]
Overall Power Health = OK
Redundancy = No

[Configuración de la política de alimentación del sistema]
System Input Power Cap = 7928 W (7928 BTU/hr | 10%)
Surplus for Peak Performance = 7000 W (6130 BTU/hr)
Redundancy Policy = None
Dynamic PSU Engagement Enabled = No

[Presupuesto de alimentación]
System Input Max Power Capacity = 0 W
Input Redundancy Reserve = 0 W
Input Power Allocated to Servers = 0 W
Input Power Allocated to Chassis Infrastructure = 51W
Total Input Power Available for Allocation = 0 W
Standby Input Power Capacity = 0 W
```

getraclog

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra las anotaciones del registro del CMC. La fecha y hora comienza a la media noche del 1.º de enero y continúa hasta que el sistema se inicia. Después del inicio del sistema, se utiliza la fecha y hora del sistema.

Uso

```
racadm getraclog [-i]
```

```
racadm getraclog [-s <registro de inicio>] [-c <cuenta>]
[-m]
```

Opciones

[Tabla A-17](#) describe las opciones del subcomando **getraclog**.

Tabla A-17. Opciones del subcomando getraclog

Abrir	Descripción
(Ninguna)	Muestra todo el registro del CMC, incluso el número de registro, la fecha y la hora, el origen y la descripción de cada suceso.
-s <registro de inicio>	Indica el registro de inicio utilizado para visualizar la información
-c <cuenta>	Especifica la cantidad máxima de entradas que se mostrarán.
-i	Muestra la cantidad de entradas del registro del CMC.
-m	Muestra una pantalla de información a la vez y pregunta al usuario si desea avanzar a la pantalla siguiente (es similar al comando more de UNIX).

 **NOTA:** Las opciones **-A** y **-o** no generan mensajes de salida adicionales y se admiten para proporcionar compatibilidad hacia atrás para secuencias existentes.

Ejemplos

```
l racadm getraclog -c 5

Apr 21 10:17:46 cmc : CMC1: active
Apr 21 10:17:46 cmc : CMC1: AC power up
Apr 21 10:17:48 cmc : CMC1: non redundant
Apr 21 12:17:48 cmc : Login success (username = root)
Apr 23 23:59:11 cmc : session close PID 3291 succeeds

l racadm getraclog -i

Total Records: 171
```

getractive

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra la fecha y la hora actualmente definidas en el CMC.

Uso

```
racadm getractive [-d] [-z]
```

Opciones

[Tabla A-18](#) describe las opciones del subcomando **getractive**.

Tabla A-18. Opciones del subcomando getractive

Opción	Descripción
(Ninguna)	Muestra la fecha y la hora por medio del mismo formato del comando date de UNIX@.
-d	Muestra la fecha y la hora como una secuencia de dígitos numéricos, en el siguiente formato: AAAAMDDhmmss.
-z	Anexa el nombre de la zona horaria activa actual a la visualización. Ejemplo: PST8PDT (Oeste de los Estados Unidos), 279 (Seúl), 329 (Sydney). Para obtener una lista de todas las zonas horarias admitidas por el CMC, escriba: <code>racadm setractive -z *</code>

Ejemplos

```
l racadm getractive

Jue 8 de dic 20:15:26 2005

l racadm getractive -z

Jue 8 de dic de 2006 20:15:29 CST6CDT

l racadm getractive -d

0051208201542.000000
```

getredundancymode

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el estado de redundancia del CMC (redundante o no redundante).

Uso

```
racadm getredundancymode
```

Ejemplo

```
racadm getredundancymode
```

```
Redundant
```

getsel

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra las entradas del registro de sucesos del sistema (SEL, también denominado registro de hardware). La pantalla de información predeterminada muestra el número de registro, la fecha y hora, el nivel de gravedad y una descripción de cada suceso.

Uso

```
racadm getsel [-i]
```

```
racadm getsel [-s <registro de inicio>] [-c <cuenta>] [-m]
```

 **NOTA:** Las opciones -A y -o no generan mensajes de salida adicionales y se admiten para proporcionar compatibilidad hacia atrás para secuencias existentes.

Opciones

[Tabla A-19](#) describe las opciones del subcomando getsel.

Tabla A-19. Opciones del subcomando getsel

Opción	Descripción
-s <registro de inicio>	Indica el registro de inicio utilizado para visualizar la información
-c <cuenta>	Proporciona la cuenta máxima de anotaciones a generar.
-i	Muestra la cantidad de entradas del registro del CMC.
-m	Muestra una pantalla de información a la vez y pregunta al usuario si desea avanzar a la pantalla siguiente (es similar al comando more de UNIX).

Ejemplo

```
1 racadm getsel -i
```

```
Total Records: 28
```

```
1 racadm getsel -s 1 -c 1
```

```
Sun Sep 16 02:51:11 2007 normal Server Blade 12 Presence module sensor for Server Blade, device inserted was asserted
```

getsensorinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el estado de los sensores especificados.

Uso

```
racadm getsensorinfo
```

Ejemplos

```
racadm getsensorinfo
```

```
<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <lectura> <unidades> <lc> <uc>
FanSpeed 1 Fan-1 OK 4768 rpm 2344 14500
FanSpeed 2 Fan-2 OK 4873 rpm 2344 14500
FanSpeed 3 Fan-3 OK 4832 rpm 2344 14500
FanSpeed 4 Fan-4 OK 4704 rpm 2344 14500
FanSpeed 5 Fan-5 OK 4833 rpm 2344 14500
FanSpeed 6 Fan-6 OK 4829 rpm 2344 14500
FanSpeed 7 Fan-7 OK 4719 rpm 2344 14500
FanSpeed 8 Fan-8 Not OK 1 rpm 2344 14500
FanSpeed 9 Fan-9 OK 4815 rpm 2344 14500
```

```
<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <lectura> <unidades> <lc> <uc>
Temp 1 Ambient_Temp OK 22 celcius N/A 40
```

```
<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <estado CA-Bueno>
PWR 1 PS-1 Online OK
PWR 2 PS-2 Online OK
PWR 3 PS-3 Online OK
PWR 4 PS-4 Slot Empty N/A
PWR 5 PS-5 Failed OK
PWR 6 PS-6 Slot Empty N/A
```

getslotname

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el nombre de una ranura determinada (indicada por medio del número de ranura) del chasis.

Uso

```
racadm getslotname -i <identificación de la ranura>
```

Opciones

[Tabla A-20](#) describe las opciones del subcomando `getslotname`.

Tabla A-20. Opciones del subcomando `getslotname`

Opción	Descripción
-i <identificación de la ranura>	Especifica la identificación de la ranura. Valores legales: 1-16

Ejemplo

```
racadm getslotname -i 1
```

```
Websvr-1
```

getssninfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información sobre una sesión de usuario activa, incluso el nombre del usuario, la dirección IP (si corresponde) y el tipo de sesión (por ejemplo, serie, SSH o Telnet), además de la fecha y hora de inicio de sesión. Las opciones permiten ver una lista de los usuarios actualmente activos o pendientes e información resumida de las tablas de sesiones. La información resumida incluye la cantidad total de sesiones para cada estado definido del administrador de sesión:

- | Válida
- | Memoria

Uso

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

Opciones

En la [tabla A-21](#) se describen las opciones del subcomando getssninfo.

Tabla A-21. Opciones del subcomando getssninfo

Opción	Descripción
-u <nombre de usuario>	Limita los resultados impresos a los registros de sesiones detallados del usuario especificado.
-u *	Si se indica un asterisco (*) como nombre de usuario, se enumerarán todos los usuarios. La información resumida no aparece cuando se elige esta opción.
-A	Suprime los encabezados y las etiquetas al brindar la información.

Ejemplos

```
| racadm getssninfo

Type           User           IP Address      Login Date/Time
SSH            root           10.9.72.252     11/28/2007 23:13:32
KVM            root           169.254.31.30   11/28/2007 18:44:51
SSH            root           10.9.72.252     11/28/2007 23:22:37

| racadm getssninfo -A

\Telnet\root\143.166.174.19\05/01/2007 02:13:59

| racadm getssninfo -A -u *

\KVM\root\169.254.31.30\11/28/2007 18:44:51
\SSH\root\10.9.72.252\11/28/2007 23:22:37
```

getsvctag

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información de la etiqueta de servicio, si existe, para uno o todos los módulos del chasis.

Uso

racadm getsvctag [-m <módulo>]

Opciones

[Tabla A-22](#) describe las opciones del subcomando `getsvctag`.

Tabla A-22. Opciones del subcomando `getsvctag`

Opción	Descripción
(Ninguna)	Muestra las etiquetas de servicio de todos los módulos del chasis (incluso del chasis).
-m <módulo>	Muestra la etiqueta de servicio del módulo especificado. El <módulo> puede estar representado por una de las siguientes opciones: <ul style="list-style-type: none"> server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6 chasis

Ejemplos

```
1 racadm getsvctag

<módulo>      <Etiqueta de servicio>
Chassis
switch-1      ABC1234
switch-2
switch-3
switch-4
switch-5
switch-6
server-1      abc123
server-2
server-3      N/A
server-4
server-5
server-6      N/A
server-7      0000014
server-8
server-9      Extension(1)
server-10     N/A
server-11     N/A
server-12
server-13     N/A
server-14
server-15     1234567
server-16     N/A

1 racadm getsvctag -m switch-1

<módulo> <Etiqueta de servicio>
switch-1 ABC1234
```

getsysinfo

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información relacionada con el CMC.

Uso

```
racadm getsysinfo [-d] [-c] [-A]
```

Opciones

Tabla A-23. Opciones del subcomando getsysinfo

Opción	Descripción
-d	Muestra información sobre el CMC.
-c	Muestra información sobre el chasis.
-A	Suprime los encabezados y las etiquetas al brindar la información.

Ejemplo

```

1 racadm getsysinfo -c

CMC Information:
CMC Date/Time           = Tue, 01 May 2007 02:33:47
Primary CMC Version     = 1.3 (Build 06.12)
Standby CMC Version     =
Last Firmware Update    = Thu, 01 May 2007 02:12:43
Hardware Version        = 15
Current IP Address       = 143.166.152.39
Current IP Gateway       = 143.166.152.1
Current IP Netmask       = 255.255.255.0
DHCP enabled            = 1
MAC Address              = 00:11:43:FD:B4:39
Current DNS Server 1    = 0.0.0.0
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP   = 0
Register DNS CMC Name   = 1
DNS CMC Name             = cmc-51186
Current DNS Domain      =

1 racadm getsysinfo -A

"CMC Information:"
"Tue, 01 May 2007 02:33:47 AM
"1.3 (Build 06.12)" "" "Thu, 01 May 2007 02:12:43" "15" "143.166.152.39" "143.166.152.1" "255.255.255.0" "1" "00:11:43:FD:B4:39"
"0.0.0.0" "0.0.0.0" "0" "1" "cmc-51186" ""

```

gettracelog

 **NOTA:** Este comando es sólo para uso interno de Dell.

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra el registro de rastreo de diagnóstico del CMC. El mensaje de salida predeterminado muestra el número de anotación, la fecha y la hora, el origen y la descripción. La fecha y hora comienza a la media noche del 1.º de enero y continúa hasta que el sistema se inicia. Durante el inicio del sistema, la fecha y la hora se muestran como <inicio del sistema>. Después del inicio del sistema, se utiliza la fecha y hora del sistema.

Uso

```

racadm gettracelog [-i]

racadm gettracelog [-s <registro de inicio>] [-c <cuenta>] [-m]

```

Opciones

[Tabla A-24](#) describe las opciones del subcomando gettracelog.

Tabla A-24. Opciones del subcomando gettracelog

Opción	Descripción
(Ninguna)	Muestra el registro de rastreo del CMC.
-s	Indica el registro de inicio que se visualizará.
-c	Especifica la cantidad de registros a visualizar.

-i	Muestra la cantidad de entradas del registro de rastreo del CMC.
-m	Muestra una pantalla de información a la vez y pregunta al usuario si desea avanzar a la pantalla siguiente (es similar al comando <code>more</code> de UNIX).

Ejemplo

```
l racadm gettracelog -c 5

Nov 28 04:40:41 cmc syslogd 1.4.1: restart.
Nov 28 04:40:41 cmc fupmuxd[150]: Start Status Op: priv=0x00000000 ID:[01 01 0x00]
Nov 28 04:40:41 cmc fupmuxd[150]: Active-CMC Status: 0x04000000
Nov 28 04:40:52 cmc webcgi[28776]: postFWUpload: rc = 10, file size = 0
Nov 28 04:40:52 cmc fupmuxd[150]: Start Status Op: priv=0x00000000 ID:[01 01 0x00]

l racadm gettracelog -i

Total Records: 275
```

help y help <comando>

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

El comando **help** muestra una lista de todos los subcomandos que pueden utilizarse con el comando `racadm` y brinda una breve descripción de cada uno.

Con **help <comando>** es posible acceder a la sintaxis del comando especificado.

 **NOTA:** También pueden utilizarse los comandos `? y ? <comando>` para obtener la misma información.

Uso

```
racadm help
```

```
racadm help <subcomando>
```

Ejemplos

```
l racadm help getsysinfo

getsysinfo -- display general CMC and system information

Usage:
racadm getsysinfo [-d] [-c] [-A]

-d : show CMC information
-c : show chassis information
-A : do not show headers or labels
```

ifconfig

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Muestra información de la interfaz de red.

Uso

```
racadm ifconfig
```

Ejemplos

```
racadm ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:55:AB:39:10:0F
          inet addr:10.35.155.160  Bcast:10.35.155.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:457405 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16321 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:51383270 (49.0 MiB)  TX bytes:6573645 (6.2 MiB)
```

netstat

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Muestra las estadísticas de red y tabla de enrutamiento.

Uso

```
racadm netstat
```

Ejemplos

```
racadm netstat
```

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
10.35.155.0 * 255.255.255.0 U 0 0 0 eth0
predeterminado 10.35.155.1 0.0.0.0 UG 0 0 0 eth0
```

ping

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Envía paquetes de eco ICMP a un destino en la red.

Uso

```
racadm ping <dirección IP>
```

Ejemplos

```
racadm ping 10.9.72.252
```

```
PING 10.9.72.252 (10.9.72.252): 56 data bytes
64 bytes from 10.9.72.252: icmp_seq=0 ttl=121 time=2.9 ms

--- 10.9.72.252 ping statistics ---
1 packets transmitted, 1 packets received, 0 percent packet loss
round-trip min/avg/max = 2.9/2.9/2.9 ms
```

racdump

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Muestra información completa del estado de configuración y del estado del chasis, así como también registros de eventos históricos. Se usa para realizar una verificación de la configuración después de la instalación y durante las sesiones de depuración de errores.

Racdump incluye los siguientes subsistemas e incorpora los siguientes comandos de RACADM:

Subsistema	Comando de RACADM
Información general del sistema/RAC	getsysinfo
Información de la sesión	getssinfo
Información del sensor	getsensorinfo
Intercambia información (módulo de E/S)	getioinfo
Información de la tarjeta intermedia (tarjeta subordinada)	getdcinfo
Información de todos los módulos	getmodinfo
Información del presupuesto de alimentación	getpbinfo
Información de KVM	getkvminfo
Información del NIC (módulo CMC)	getniccfg
Información de redundancia	getredundancymode
Información del registro de rastreo	gettracelog
Registro de sucesos de RAC	gettraclog
Registro de sucesos del sistema	getsel

Uso

```
racadm racdump
```

Ejemplo

```
racadm racdump
```

```
=====
General System/RAC Information
=====

CMC Information:
CMC Date/Time           = Wed, 28 Nov 2007 11:55:49 PM
Primary CMC Version     = X08
Standby CMC Version     = N/A
Last Firmware Update    = Wed Nov 21 21:37:56 2007
Hardware Version        = 2
Current IP Address      = 10.35.155.160
Current IP Gateway      = 10.35.155.1
Current IP Netmask      = 255.255.255.0
DHCP Enabled           = 1
MAC Address             = 00:55:AB:39:10:0F
Current DNS Server 1    = 0.0.0.0
Current DNS Server 2    = 0.0.0.0
DNS Servers from DHCP  = 0
Register DNS CMC Name   = 0
DNS CMC Name           = cmc-servicetag
Current DNS Domain     =

Chassis Information:
System Model            = PowerEdgeM1000eControlPanel
System AssetTag         = 00000
Service Tag             =
Chassis Name            = Dell Rack System
Chassis Location        = [UNDEFINED]
Power Status            = ON

=====
Session Information
=====

Type User IP Address Login Date/Time
SSH root 10.9.72.252 11/28/2007 23:40:53
KVM root 169.254.31.30 11/28/2007 18:44:51

=====
Sensor Information
=====

<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <lectura> <unidades> <lc> <uc>
FanSpeed 1 Fan-1 OK 14495 rpm 7250 14500
FanSpeed 2 Fan-2 OK 14505 rpm 7250 14500
```

```
FanSpeed 3 Fan-3 OK 4839 rpm 2344 14500
FanSpeed 4 Fan-4 OK 14527 rpm 7250 14500
FanSpeed 5 Fan-5 OK 14505 rpm 7250 14500
FanSpeed 6 Fan-6 OK 4835 rpm 2344 14500
FanSpeed 7 Fan-7 OK 14521 rpm 7250 14500
FanSpeed 8 Fan-8 Not OK 1 rpm 7250 14500
FanSpeed 9 Fan-9 OK 4826 rpm 2344 14500
```

```
<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <lectura> <unidades> <lc> <uc>
Temp 1 Ambient_Temp OK 21 celcius N/A 40
```

```
<Tipo de sensor> <Núm.> <Nombre de sensor> <estado> <estado CA-Bueno>
WR 1 PS-1 Online OK
PWR 2 PS-2 Online OK
PWR 3 PS-3 Online OK
PWR 4 PS-4 Slot Empty N/A
PWR 5 PS-5 Failed OK
PWR 6 PS-6 Slot Empty N/A
```

racreset

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Activa un restablecimiento ordenado o forzado del CMC. El suceso de restablecimiento se escribe en el registro del CMC. Cuando este comando se ejecuta sin la opción **hard**, **racreset** ejecuta un restablecimiento ordenado. El restablecimiento forzado realiza una operación de restablecimiento profunda en el CMC. Por lo tanto, sólo debe utilizarse como último recurso para recuperar el CMC.

-  **AVISO:** Después de ejecutar un restablecimiento forzado del CMC es necesario reiniciar el sistema. Consulte el apartado [racreset](#).
-  **AVISO:** Cuando se ejecuta un subcomando **racreset**, es posible que el CMC tarde hasta un minuto para volver a un estado utilizable.

Uso

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

Opciones

En la [tabla A-25](#) se describen las opciones del subcomando **racreset**.

Tabla A-25. Opciones del subcomando racreset

Opción	Descripción
hard	El restablecimiento <i>forzado</i> realiza una operación de restablecimiento profundo en el controlador de acceso remoto. Esta opción sólo debe utilizarse como último recurso para fines de recuperación del CMC.
soft	El restablecimiento <i>ordenado</i> realiza una operación de reinicio ordenado en CMC.

Ejemplo

```
1 racadm racreset
```

Ejecuta una secuencia de restablecimiento ordenado en el CMC.

```
1 racadm racreset soft
```

Ejecuta una secuencia de restablecimiento ordenado en el CMC.

```
1 racadm racreset hard
```

Ejecuta una secuencia de restablecimiento forzado en el CMC.

racresetcfg

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

 **NOTA:** Apague el chasis antes de ejecutar este comando.

Descripción

Elimina todas las entradas de propiedades de base de datos del CMC o el iKVM y restaura la configuración predeterminada de fábrica. Después de restaurar las propiedades de base de datos, el CMC se restablece de forma automática. El iKVM también se restablece de forma automática cuando el comando `racresetcfg` se utiliza para restaurar las propiedades predeterminadas.

 **AVISO:** Este comando elimina la configuración actual del CMC y restablece los valores predeterminados originales de la configuración serie y del CMC. Después del restablecimiento, el nombre y la contraseña predeterminados serán `root` y `calvin` respectivamente, y la dirección IP será `192.168.0.120`. Si emite el comando `racresetcfg` desde un cliente de red (por ejemplo, un explorador de web o Telnet/SSH compatible), deberá utilizar la dirección IP predeterminada.

Uso

```
racadm racresetcfg [-m <módulo>]
```

Opciones

[Tabla A-26](#) describe las opciones del subcomando `racresetcfg`.

Tabla A-26. Opciones del subcomando `racresetcfg`

Opción	Descripción
-m <módulo>	<p>Especifica el módulo cuyas propiedades de base de datos se desean restablecer.</p> <p>El <módulo> puede ser cualquiera de las siguientes opciones:</p> <ul style="list-style-type: none"> chasis kvm server-<i>n</i> donde <i>n</i>=1 - 16 <p>Valor predeterminado: chasis</p>

Ejemplo

```
racadm racresetcfg -m kvm
```

The configuration has initiated restoration to factory defaults. (La configuración ha iniciado el proceso de restauración de los valores predeterminados.)

serveraction

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Ejecuta el restablecimiento, encendido, apagado o ciclo de encendido del servidor especificado.

Uso

```
racadm serveraction [-m <server-n>] <acción>
```

```
racadm serveraction [-a] <acción>
```

Opciones

[Tabla A-27](#) describe las opciones del subcomando `serveraction`.

Tabla A-27. Opciones del subcomando `serveraction`

--	--

Opción	Descripción
-m server- <i>n</i>	Especifica el servidor por medio del número de ranura (1-16) correspondiente en el chasis. Ejemplo: server-2.
-a	La acción de alimentación especificada se realiza en todos los servidores
<acción>	Especifica la acción. La <acción> puede estar representada por una de las siguientes opciones: <ul style="list-style-type: none"> powerdown: apaga el servidor. powerup: enciende el servidor. powercycle: ejecuta una operación de ciclo de encendido en el servidor. hardreset: ejecuta una operación de restablecimiento (reinicio) en el servidor. graceshutdown: apaga el servidor de forma ordenada. powerstatus: muestra el estado de alimentación actual (ya sea en línea o sin conectar) del servidor.

Ejemplo

```

I racadm serveraction -m server-1 powerup

Server power operation successful.

(La operación de encendido del servidor se realizó correctamente.)

I racadm serveraction -m server-9 powerup

ERROR: Server in slot 9 is an extension of the server in slot 1.

(ERROR: el servidor en la ranura 9 es una extensión del servidor en la ranura 1.)

```

setchassisname

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define el nombre del chasis en la pantalla LCD.

Uso

```
racadm setchassisname <nombre>
```

Ejemplo

```

racadm setchassisname dellchassis-1

The chassis name was set successfully.

(El nombre del chasis se definió correctamente.)

```

setassettag

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define la etiqueta de propiedad ASCII de N bytes del chasis.

Uso

```
racadm setassettag -m chassis <etiqueta de propiedad>
```

Opciones

[Tabla A-28](#) describe las opciones del subcomando `setassettag`.

Tabla A-28. Opciones del subcomando `setassettag`

Opción	Comando
<code>-m <módulo></code>	Especifica el módulo cuya etiqueta de propiedad se desea establecer. Valor legal: chassis NOTA: Dado que existe un único valor legal, puede obtenerse la misma información aun sin incluir esta opción.

Ejemplo

Datos de entrada:

```
racadm setassettag -m chassis 783839-33
```

O bien:

```
racadm setassettag 783839-33
```

The asset tag was changed successfully.

(La etiqueta de propiedad se modificó satisfactoriamente.)

setflexaddr

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Activa o desactiva FlexAddress en una ranura/estructura de red en particular.

 **NOTA:** Si se determina que el tipo de estructura de red es Infiniband, la operación se cancela y el comando muestra un error. Si la función FlexAddress no está activada, el comando mostrará un error.

 **NOTA:** Se debe apagar el servidor para cambiar el estado de la ranura. Se deben apagar todos los servidores para cambiar el estado de la estructura de red.

Uso

```
racadm setflexaddr [-i <N° ranura> <estado>]  
[-f <nombre de estructura de red> <estado>]
```

<N° ranura> = 1 a 16

<nombre de estructura de red> = A, B, C

<estado> = 0 o 1

donde 0 es desactivar y 1 es activar

Opciones

[Tabla A-29](#) describe las opciones del subcomando `setflexaddr`.

Tabla A-29. Opciones del subcomando `setflexaddr`

Opción	Descripción
<code>-i <N° ranura> <estado></code>	Activa o desactiva FlexAddress para la ranura especificada.

`-f <nombre de estructura de red> <estado>` Activa o desactiva FlexAddress para la estructura de red especificada.

Ejemplo

```
l racadm setflexaddr -i 1 0
Slot 1 FlexAddress state set successfully
(Estado de FlexAddress de la Ranura 1 configurado satisfactoriamente)
l racadm setflexaddr -f A 1
Fabric A FlexAddress state set successfully
(Estado de FlexAddress de la Estructura de red A configurado satisfactoriamente)
```

setled

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define el estado (parpadeando o sin parpadear) del indicador LED del módulo especificado.

Uso

```
racadm setled -m <módulo> -l <estado del LED>
```

Opciones

[Tabla A-30](#) describe las opciones del subcomando **setled**.

Tabla A-30. Opciones del subcomando setled

Opción	Descripción
-m <módulo>	Especifica el módulo cuyo indicador LED se desea configurar. El <módulo> puede ser una de las siguientes opciones: <ul style="list-style-type: none">l server-<i>n</i> donde <i>n</i>=1-16l switch-<i>n</i> donde <i>n</i>=1-6l cmc-activel chassis
-l <estado_del_LED>	Especifica si el indicador LED debe parpadear. El <estado_del_LED> puede ser una de las siguientes opciones: <ul style="list-style-type: none">l 0: sin parpadearl 1: parpadeando

Ejemplo

```
l racadm setled -m server-1 -l 1
LED state was set successfully.
(El estado del LED se estableció satisfactoriamente.)
l racadm setled -m server-9 -l 1
ERROR: Server in slot 9 is an extension of the server in slot 1.
(ERROR: el servidor en la ranura 9 es una extensión del servidor en la ranura 1.)
```

setniccfg

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define la configuración de IP del módulo especificado.

Uso

```
racadm setniccfg [-m <módulo>] [-d] [-o] [-s <dirección_IP> <máscara_de_subred> <puerta_de_enlace>] [-k <velocidad> <dúplex>]
```

```
racadm setniccfg [-m <módulo>] -d
```

```
racadm setniccfg [-m <módulo>] -s <dirección_IP> <máscara_de_red> <puerta_de_enlace>
```

```
racadm setniccfg [-m <módulo>] -o
```

```
racadm setniccfg [-m <módulo>] -k [<velocidad> <dúplex>]
```

Opciones

[Tabla A-31](#) describe las opciones del subcomando **setniccfg**.

Tabla A-31. Opciones del subcomando setniccfg

Opción	Descripción
-m <módulo>	Indica el módulo para el que se desea establecer la configuración de IP. El <módulo> puede ser cualquiera de las siguientes opciones: <ul style="list-style-type: none"> server-<i>n</i> donde <i>n</i>=1-16 switch-<i>n</i> donde <i>n</i>=1-6 chassis Si se excluye la opción -m, el valor predeterminado del módulo será chassis.
-d	Activa el DHCP para el puerto de administración de Ethernet (el valor predeterminado es DHCP activado).
-s	Permite definir la configuración de IP estática mediante la especificación de la dirección IP, la máscara de subred y la puerta de enlace. <dirección_IP>, <máscara_de_red> y <puerta_de_enlace> se deben escribir como cadenas separadas con puntos. Si no se suministran valores para esta opción, se utilizará la configuración estática ya existente.
-o	Desactiva por completo el puerto de administración de Ethernet.
-k	Especifica la velocidad y el dúplex para la tarjeta de interfaz de red. <ul style="list-style-type: none"> Velocidad: 10, 100 Dúplex: medio, completo (sin un valor especificado): negociación automática

Ejemplos

```
| racadm setniccfg -m server-1 143.166.152.39 143.166.152.1 255.255.255.0  
  
OK (En buen estado)  
  
| racadm setniccfg -m server-9 143.166.152.39 143.166.152.1 255.255.255.0  
  
ERROR: Server in slot 9 is an extension of the server in slot 1.  
  
(ERROR: el servidor en la ranura 9 es una extensión del servidor en la ranura 1.)  
  
| racadm setniccfg -k 100 full  
  
Speed and Duplex settings modified successfully.
```

(La configuración de velocidad y de dúplex se modificó satisfactoriamente.)

setractime

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define la fecha y la hora en el CMC.

Uso

```
racadm setractime -d <yyyymmddhhmmss.mmmmmsoff>
```

```
racadm setractime -l <yyyymmddhhmmss> [-z <zona>]
```

Opciones

[Tabla A-32](#) describe las opciones del subcomando **setractime**.

Tabla A-32. Opciones del subcomando **setractime**

Opción	Descripción
-d	Define la hora en la cadena de caracteres <i>yyyymmddhhmmss.mmmmmsoff</i> , donde: <ul style="list-style-type: none"> <i>yyyy</i> representa el año <i>mm</i> representa el mes <i>dd</i> representa el día <i>hh</i> representa la hora <i>mm</i> representa los minutos <i>ss</i> representa los segundos <i>mmmmmm</i> representa la cantidad de microsegundos <i>s</i> puede ser un signo + (más) o - (menos), lo que indica el signo de compensación <i>off</i> representa la compensación expresada en minutos <p>NOTA: El valor <i>off</i> representa la compensación expresada en minutos desde la hora GMT, en incrementos de 15 minutos.</p>
-z <zona>	Establece la zona horaria. Ejemplo: PST8PDT (Oeste de los Estados Unidos), 279 (Seúl), 329 (Sydney). Para ver una lista de zonas horarias, escriba el siguiente comando: <pre>racadm setractime -z *</pre>
-l	Define la fecha y hora locales en la cadena <i>yyyymmddhhmmss</i> , donde: <ul style="list-style-type: none"> <i>yyyy</i> representa el año <i>mm</i> representa el mes <i>dd</i> representa el día <i>hh</i> representa la hora <i>mm</i> representa los minutos <i>ss</i> representa los segundos <p>NOTA: Es recomendable configurar la hora a través de las opciones -l y -z. Este formato de comando permite que el CMC admita por completo las zonas horarias locales, incluyendo la habilidad para ajustar automáticamente la hora del CMC al horario de verano local.</p>

Ejemplo

El subcomando **setractime** admite fechas desde 1/1/1970 00:00:00 a 12/31/2030 23:59:59. Para definir la fecha como 24 de octubre de 2007 a las 15:02:30 horas del horario estándar de la costa Pacífico de los EE.UU.:

```
racadm setractime -l 20071024150230 -z PST8PDT
```

The time was set successfully.

(La hora se definió correctamente.)

setslotname

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

 **NOTA:** Consulte [Edición de los nombres de ranuras](#) para ver las reglas para seleccionar nombres de ranuras.

Descripción

Establece el nombre de una ranura en el chasis.

Uso

```
racadm setslotname -i <identificación de ranura> <nombre de ranura>
```

Opciones

[Tabla A-33](#) describe las opciones del subcomando **setslotname**.

Tabla A-33. Opciones del subcomando **setslotname**

Opción	Descripción
<identificación de ranura>	Indica la ubicación de la ranura en el chasis. Valores legales: 1-16
<nombre_de_ranura>	Indica el nuevo nombre que se asignará a la ranura.

Ejemplo

```
racadm setslotname -i 3 mserver3
```

The slot name was set successfully.

(El nombre de la ranura se asignó correctamente.)

setsysinfo

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Define el nombre o la ubicación del chasis.

Uso

```
racadm setsysinfo [-c chassisname|chassislocation] <cadena>
```

Opción

[Tabla A-34](#) describe las opciones del subcomando **setsysinfo**.

Tabla A-34. Opciones del subcomando **setsysinfo**

Opción	Descripción
<cadena>	Indica el nombre o la ubicación del chasis en ASCII de N bytes.

Ejemplo

```
racadm setsysinfo -c chassisname "Dell Rack System"
```

The chassis name was set successfully.

(El nombre del chasis se definió correctamente.)

sslcertdownload

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

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

Uso

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

Opciones

En la [tabla A-35](#) se describen las opciones del subcomando **sslcertdownload**.

Tabla A-35. Opciones del subcomando sslcertdownload

Opción	Descripción
-t	Especifica el tipo de certificado que se desea descargar: 1: certificado del servidor 2: certificado de Microsoft Active Directory
-f	Especifica la ruta de acceso local y el nombre del archivo donde se guardará el certificado.

Restricciones

El subcomando **sslcertdownload** sólo puede ejecutarse desde un cliente remoto.

Ejemplo

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

Certificate successfully downloaded from the CMC.

(El certificado se descargó satisfactoriamente del CMC.)

sslcertupload

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Permite cargar en el CMC un certificado de servidor SSL personalizado o firmado por una autoridad de certificados desde el cliente.

Uso

```
racadm sslcertupload -t <tipo> -f <nombre de archivo>
```

Opciones

En la [tabla A-36](#) se describen las opciones del subcomando **sslcertupload**.

Tabla A-36. Opciones del subcomando sslcertupload

Opción	Descripción
-t <tipo>	Especifica el tipo de certificado que se va a cargar: 1: certificado del servidor 2: certificado firmado por una autoridad de certificados
-f <nombre de archivo>	Especifica el nombre de archivo del certificado que se va a cargar.

Restricciones

El subcomando **sslcertupload** sólo puede ejecutarse desde un cliente local.

Ejemplo

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

Certificate successfully uploaded to the CMC.

(El certificado se cargó satisfactoriamente en el CMC.)

sslcertview

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador**.

Descripción

Muestra el certificado de servidor SSL, o firmado por una autoridad de certificados, que se encuentra en el CMC.

Uso

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

Opciones

En la [tabla A-37](#) se describen las opciones del subcomando **sslcertview**.

Tabla A-37. Opciones del subcomando sslcertview

Opción	Descripción
-t <tipo>	Especifica el tipo de certificado que se va a descargar, ya sea un certificado de Microsoft Active Directory o un certificado de servidor. 1: certificado del servidor 2: certificado de Microsoft Active Directory
-A	Suprime los encabezados y las etiquetas al brindar la información.

Restricciones

El subcomando `sslcertupload` sólo puede ejecutarse desde un cliente local.

Ejemplos

```
racadm sslcertview -t 1
```

```
Serial Number          : 00

Subject Information:
Country Code (CC)     : US
Locality (L)          : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : OpenCMC Group
Common Name (CN)      : CMCdefault

Issuer Information:
Country Code (CC)     : US
Locality (L)          : Round Rock
Organization (O)       : Dell Inc.
Organizational Unit (OU) : OpenCMC Group
Common Name (CN)      : CMCdefault

Valid From             : Nov  6 01:23:03 2007 GMT
Valid To               : Nov  3 01:23:03 2017 GMT
```

sslcsrgen

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Permite generar y descargar una solicitud de firma de certificado (CSR) SSL del CMC a la estación de administración o red compartida. La solicitud CSR puede utilizarse para crear un certificado SSL personalizado para las transacciones realizadas en el CMC.

Uso

```
racadm sslcsrgen [-g]
racadm sslcsrgen [-g] [-f <nombre de archivo>]
racadm sslcsrgen [-s]
```

Opciones

En la [tabla A-38](#) se describen las opciones del subcomando `sslcsrgen`.

Tabla A-38. Opciones del subcomando `sslcsrgen`

Opción	Descripción
-g	Genera una nueva CSR. La opción <code>-g</code> no puede utilizarse con la opción <code>-s</code> .
-s	Indica el estado del proceso de generación de la CSR: <ul style="list-style-type: none"> La CSR se generó de manera satisfactoria. La CSR no existe. Generación de la CSR en progreso. La opción <code>-s</code> no puede utilizarse con la opción <code>-g</code> .
-f <nombre de archivo>	Indica el nombre del archivo donde se descargará la CSR. Sólo puede utilizarse con la opción <code>-g</code> .

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

 **NOTA:** Si no se especifican opciones, se generará una CSR y se descargará en el sistema local de archivos como `sslcsr` de manera predeterminada.

Restricciones

El subcomando `sslcsrgen` sólo puede ejecutarse desde un cliente local y no puede utilizarse en la interfaz serie, Telnet o SSH.

Ejemplo

```
1 racadm sslcsrgen -s
CSR generation in progress.
(Generación de la CSR en progreso.)
1 racadm sslcsrgen -g -f c:\csr\csrtest.txt
The csr was generated successfully.
(La CSR se generó correctamente.)
```

sslresetcfg

 **NOTA:** Para utilizar este subcomando, debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Vuelve a generar el certificado autofirmado utilizado por el CMC de Web GUI. El certificado se activa 30 segundos después de que se haya introducido el comando.

Uso

```
racadm sslresetcfg
```

Ejemplo

```
1 racadm sslresetcfg
Certificate generated successfully and webserver restarted.
(Certificado generado satisfactoriamente y servidor web reiniciado.)
```

Tabla A-39. Opciones del subcomando `sslcsrgen`

Opción	Descripción
-g	Genera una nueva CSR. La opción <code>-g</code> no puede utilizarse con la opción <code>-s</code> .
-s	Indica el estado del proceso de generación de la CSR: <ul style="list-style-type: none">1 La CSR se generó de manera satisfactoria.1 La CSR no existe.1 Generación de la CSR en progreso. La opción <code>-s</code> no puede utilizarse con la opción <code>-g</code> .
-f <nombre de archivo>	Indica el nombre del archivo donde se descargará la CSR. Sólo puede utilizarse con la opción <code>-g</code> .

testemail

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario de alertas de prueba**.

Descripción

Envía un mensaje de correo electrónico de prueba desde el CMC a un destino determinado.

 **NOTA:** Este comando sólo es válido si las alertas por correo electrónico están activadas en el CMC. Para obtener más información sobre las alertas por correo electrónico, consulte [Configuración de alertas por correo electrónico](#).

Uso

```
racadm testemail -i <índice>
```

Opción

En la [tabla A-40](#) se describen las opciones del subcomando **testemail**.

Tabla A-40. Opciones del subcomando testemail

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

Ejemplo

```
racadm testemail -i 1
```

```
Test email sent successfully.
```

(El mensaje de correo electrónico de prueba se envió correctamente.)

testtrap

 **NOTA:** Para utilizar este subcomando debe contar con privilegios de **Usuario de alertas de prueba**.

Descripción

Comprueba la función de alerta de captura SNMP mediante el envío de una captura de prueba desde el CMC a un receptor determinado en la red.

 **NOTA:** Este comando sólo es válido si las alertas de SNMP están activadas en el CMC. Para obtener más información sobre las alertas de SNMP, consulte [Cómo configurar alertas SNMP](#).

Uso

```
racadm testtrap -i <índice>
```

Opciones

En la [tabla A-41](#) se describen las opciones del subcomando **testtrap**.

Tabla A-41. Opciones del subcomando testtrap

Opción	Descripción
-i <índice>	Especifica el índice de la configuración de captura que se utilizará para realizar la prueba. Valores legales: 1-4

Ejemplo

```
racadm testtrap -i 4
```

```
Test trap sent successfully.
```

(La captura de prueba se envió correctamente.)

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso del CMC con Microsoft Active Directory

Guía del usuario

- [Extensiones de esquemas de Active Directory](#)
- [Descripción general del esquema ampliado](#)
- [Generalidades del esquema estándar de Active Directory](#)
- [Preguntas más frecuentes](#)

Un servicio de directorio mantiene una base de datos común con toda la información necesaria para controlar los usuarios, equipos, impresoras y otros componentes de la red. Si su empresa utiliza el software de servicio Microsoft® Active Directory®, puede configurarlo para acceder al CMC. Esto le permitirá agregar y controlar privilegios de usuario del CMC a los usuarios ya existentes en el software Active Directory.

 **NOTA:** El uso de Active Directory para reconocer a los usuarios del CMC se admite en los sistemas operativos Microsoft Windows® 2000 y Windows Server® 2003.

Extensiones de esquemas de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios al CMC mediante dos métodos:

- 1 La solución del esquema ampliado, que utiliza objetos de Active Directory definidos por Dell.
- 1 El esquema estándar, que sólo utiliza objetos de grupo de Active Directory.

Esquema ampliado y esquema estándar

Si utiliza Active Directory para configurar el acceso al CMC, deberá elegir el esquema ampliado o el esquema estándar.

Con la solución de esquema ampliado:

- 1 Todos los objetos de control de acceso se mantienen en Active Directory.
- 1 La configuración del acceso de los usuarios a diferentes CMC y con distintos niveles de privilegios brinda máxima flexibilidad.

Con la solución de esquema estándar:

- 1 No se requiere una ampliación del esquema porque el esquema estándar sólo utiliza objetos de Active Directory.
 - 1 La configuración de Active Directory es sencilla.
-

Descripción general del esquema ampliado

Hay dos maneras de activar el esquema ampliado de Active Directory:

- 1 Mediante el uso de la interfaz web del CMC. Para obtener instrucciones, consulte [Configuración del CMC con Active Directory de esquema ampliado y la interfaz web](#).
- 1 Mediante el uso de la herramienta de CLI de RACADM. Para obtener instrucciones, consulte [Configuración del CMC con Active Directory de esquema ampliado y RACADM](#).

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos.

Un ejemplo de las clases almacenadas en la base de datos es la *clase user*. Los atributos de esta clase pueden incluir el nombre, apellido, número de teléfono y otros datos del usuario.

La base de datos de Active Directory puede ampliarse mediante la incorporación de atributos y clases propios y exclusivos que respondan a las necesidades específicas del entorno de su empresa. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autenticación y autorización de administración remota.

Cada atributo o clase que es se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para conservar la exclusividad de las identificaciones en toda la industria, Microsoft mantiene una base de datos de identificadores de objetos (OID) de Active Directory. Para ampliar el esquema de Active Directory, Dell estableció identificadores de objetos únicos, extensiones de nombre únicas e identificaciones de atributos vinculadas de manera exclusiva para los atributos y clases específicos de Dell:

Extensión de Dell: dell

OID base de Dell: 1.2.840.113556.1.8000.1280

Rango de identificaciones vinculadas del RAC: 12070-2079

Descripción de las extensiones de esquema de RAC

Dell proporciona un grupo de propiedades que pueden configurarse. El esquema ampliado de Dell incluye propiedades de asociación, dispositivos y privilegios.

La propiedad de asociación vincula a usuarios o grupos con un conjunto específico de privilegios para uno o más dispositivos de RAC. Este modelo proporciona al administrador la máxima flexibilidad sobre las combinaciones diferentes de usuarios, privilegios de RAC y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción general de los objetos de Active Directory

Si existen dos CMC en la red que se desean integrar a Active Directory para su autenticación y autorización, será necesario crear al menos un objeto de asociación y un objeto de dispositivo de RAC para cada CMC. Puede crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios, grupos de usuarios u objetos de dispositivo de RAC sean necesarios. Los usuarios y objetos de dispositivo de RAC pueden ser miembros de cualquier dominio en la empresa.

Sin embargo, cada objeto de asociación puede ser vinculado (o, puede unir usuarios, grupos de usuarios u objetos de dispositivo de RAC) a sólo un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los CMC específicos.

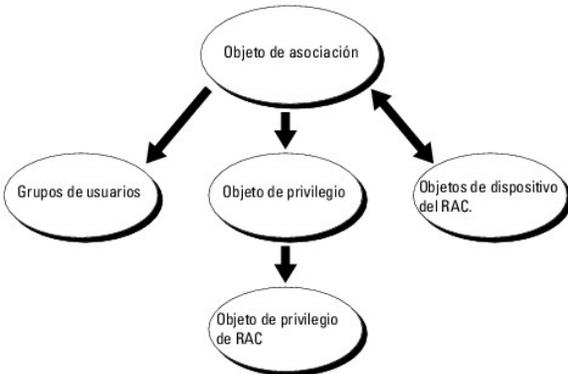
El objeto del dispositivo del RAC es el eslabón al firmware de RAC para consultar a Active Directory para la autenticación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autenticación y la autorización con Active Directory. Además, el administrador también debe agregar el sistema a por lo menos un objeto de asociación para que los usuarios se puedan autenticar.

La [figura 7-1](#) muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

NOTA: El objeto de privilegio de RAC se aplica al DRAC 4, el DRAC 5 y el CMC.

Pueden crearse tantos objetos de asociación como sea necesario. No obstante, es necesario crear al menos un objeto de asociación y disponer de un objeto de dispositivo de RAC para cada RAC (CMC) de la red que se desee integrar a Active Directory.

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

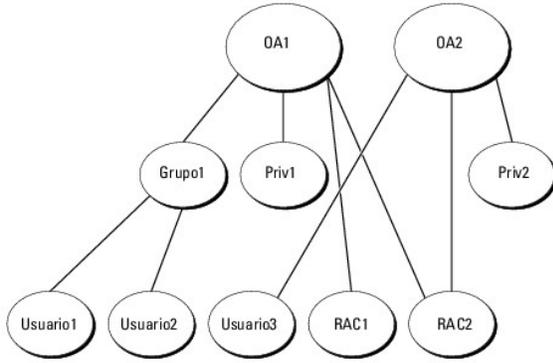


El objeto de asociación permite esta cantidad de usuarios y/o grupos así como objetos de dispositivo de RAC. Sin embargo, el objeto de asociación sólo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los "usuarios" con "privilegios" en los RAC (CMC).

Además, se pueden configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, supongamos que tiene dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3). Usted desea otorgar privilegios de administrador para ambos CMC a los usuarios 1 y 2, y privilegios de inicio de sesión a la tarjeta de RAC2 para el usuario3. [Figura 7-2](#) muestra cómo configurar los objetos de Active Directory en este escenario.

Cuando se agregan grupos universales a partir de dominios independientes, se debe crear un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados creados por la utilidad Dell Schema Extender, son grupos locales de dominio y no funcionarán con grupos universales de otros dominios.

Figura 7-2. Configuración de objetos de Active Directory en un solo dominio



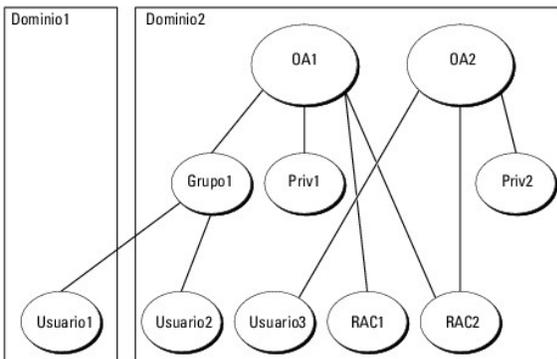
Cómo configurar los objetos para un solo dominio:

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representarán a los dos CMC.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (de administrador) y Priv2 tiene privilegio de inicio de sesión.
4. Agrupe al usuario1 y usuario2 en el Grupo1.
5. Agregue el Grupo1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objetos de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC también en A01.
6. Agregue el usuario3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objetos de privilegio en A02, y RAC2 como dispositivo de RAC también en A02.

Para obtener una instrucción detallada, consulte [Cómo agregar usuarios y privilegios del CMC a Active Directory](#).

La [figura 7-3](#) muestra un ejemplo de los objetos de Active Directory en varios dominios. En este escenario, existen dos CMC (RAC1 y RAC2) y tres usuarios 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 para ambos CMC, y el usuario3 con privilegios de inicio de sesión para la tarjeta de RAC2.

Figura 7-3. Configuración de objetos de Active Directory en múltiples dominios



Cómo configurar los objetos para varios dominios:

1. Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2. Cree dos objetos de asociación, A01 (de ámbito universal) y A02, en cualquier dominio.
La [figura 7-3](#) muestra los objetos en el Dominio2.
3. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representarán a los dos CMC.
4. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (de administrador) y Priv2 tiene privilegio de inicio de sesión.
5. Agrupe al usuario1 y usuario2 en el Grupo1. El ámbito de grupo del Grupo1 debe ser Universal.
6. Agregue el Grupo1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objetos de privilegio en A01, y RAC1 y RAC2 como dispositivos de

RAC también en A01.

7. Agregue el usuario3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objetos de privilegio en A02, y RAC2 como dispositivo de RAC también en A02.

Configuración de Active Directory con esquema ampliado para acceder al CMC

Antes de utilizar Active Directory para acceder al CMC, debe configurar el software Active Directory y el CMC:

1. Amplíe el esquema de Active Directory (consulte [Extensión del esquema de Active Directory](#)).
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte [Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory](#)).
3. Agregue usuarios de CMC y sus privilegios a Active Directory (consulte [Cómo agregar usuarios y privilegios del CMC a Active Directory](#)).
4. Active SSL en cada uno de los controladores de dominio.
5. Configure las propiedades de Active Directory de CMC por medio de la interfaz web del CMC o la RACADM (consulte [Configuración del CMC con Active Directory de esquema ampliado y la interfaz web](#) o [Configuración del CMC con Active Directory de esquema ampliado y RACADM](#)).

Extensión del esquema de Active Directory

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, asegúrese de contar con privilegios de administrador de esquema en el titular de las funciones de operaciones de maestro único flexible (FSMO) de maestro de esquema del bosque de dominio.

Puede ampliar el esquema por medio de uno de los métodos siguientes:

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

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation*, en los siguientes directorios respectivamente:

- 1 <unidad de DVD>:\SYSMGMT\ManagementStation\support\
OMActiveDirectory_Tools\<tipo de instalación>\LDIF Files
- 1 <unidad de DVD>:\SYSMGMT\ManagementStation\support\
OMActiveDirectory_Tools\<tipo de instalación>\Schema Extender

Para usar los archivos LDIF, consulte las instrucciones en el archivo readme (léame) que está en el directorio **LDIF_Files**. Para obtener instrucciones sobre el uso de Dell Schema Extender para ampliar el Esquema de Active Directory, consulte "[Uso del amplificador de esquema de Dell](#)".

Puede copiar y ejecutar el amplificador de esquema o los archivos LDIF desde cualquier ubicación.

Uso del amplificador de esquema de Dell



AVISO: Dell Schema Extender utiliza el archivo **SchemaExtenderOem.ini**. Para asegurar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
2. Lea y comprenda la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar el amplificador de esquema de Dell.
5. Haga clic en **Finish (Finalizar)**.

El esquema ha sido extendido. Para verificar la ampliación del esquema, utilice la Consola de administración de Microsoft (MMC) y el complemento Esquema de Active Directory para controlar que existan los siguientes elementos:

- 1 Clases: consulte de [tabla 7-1](#) a [tabla 7-6](#)
- 1 Atributos: consulte [tabla 7-7](#)

Consulte la documentación de Microsoft para obtener más información acerca de cómo activar y utilizar el complemento Esquema de Active Directory en

MMC.

Tabla 7-1. Definiciones de clases para las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 7-2. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Descripción	Representa el dispositivo RAC de Dell. El dispositivo RAC debe estar configurado como dellRacDevice en Active Directory. Esta configuración permite al CMC enviar consultas de Protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 7-3. 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
SuperClasses	Grupo
Atributos	dellProductMembers dellPrivilegeMember

Tabla 7-4. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los derechos de autorización (privilegios) para el dispositivo CMC.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabla 7-5. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Clase que contiene los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 7-6. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
-----	------------------------------------

Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 7-7. Lista de atributos agregados al esquema de Active Directory

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: dellPrivilegeMember Descripción: lista de los objetos dellPrivilege pertenecientes a este atributo. OID: 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
Atributo: dellProductMembers Descripción: lista de los objetos dellRacDevices pertenecientes a esta función. Este atributo es el vínculo para avanzar al vínculo dellAssociationMembers. Identificación de vínculo: 12070 OID: 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
Atributo: dellSCardConfigAdmin Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de configuración de tarjeta en el dispositivo. OID: 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
Atributo: dellSLoginUser Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de inicio de sesión en el dispositivo. OID: 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
Atributo: dellSCardConfigAdmin Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de configuración de tarjeta en el dispositivo. OID: 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
Atributo: dellSUserConfigAdmin Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de administrador de configuración de usuarios en el dispositivo. OID: 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
Atributo: dellSLogClearAdmin Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de administrador de borrado de registros en el dispositivo. OID: 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
Atributo: dellSServerResetUser Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de restablecimiento de servidor en el dispositivo. OID: 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
Atributo: dellSTestAlertUser Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de usuario de alertas de prueba en el dispositivo. OID: 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
Atributo: dellSDebugCommandAdmin Descripción: el valor que se establece es TRUE si el usuario cuenta con derechos de administrador de comandos de depuración de errores en el dispositivo.	

OID: 1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPATYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Atributo: dellSchemaVersion Descripción: se utiliza la versión de esquema actual para actualizar el esquema.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.12 Cadena que no distingue entre mayúsculas y minúsculas (LDAPATYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Atributo: dellRacType Descripción: este atributo representa el tipo de RAC actual para el objeto dellRacDevice y el vínculo de retroceso del vínculo dellAssociationObjectMembers.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.13 Cadena que no distingue entre mayúsculas y minúsculas (LDAPATYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Atributo: dellAssociationMembers Descripción: lista de los objetos dellAssociationObjectMembers pertenecientes a este producto. Este atributo es el eslabón de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	
OID: 1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPATYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Atributo: dellPermissionsMask1	
OID: 1.2.840.113556.1.8000.1280.1.6.2.1 número entero (LDAPATYPE_INTEGER)	
Atributo: dellPermissionsMask2	
OID: 1.2.840.113556.1.8000.1280.1.6.2.2 número entero (LDAPATYPE_INTEGER)	

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

Cuando se amplía el esquema en Active Directory, también debe ampliarse el complemento Usuarios y equipos de Active Directory para que el administrador pueda administrar los usuarios, dispositivos y grupos de usuarios de RAC (CMC), y las asociaciones y privilegios del RAC.

Cuando instala el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation*, puede ampliar el complemento si selecciona la opción **Extensión de Dell para el complemento de usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener más instrucciones sobre la instalación del software de administración de sistemas.

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

Instalación de Administrator Pack

Es imprescindible instalar el paquete de administrador en cada sistema que administra los objetos del CMC de Active Directory. Si no instala Administrator Pack, no podrá ver el objeto RAC de Dell en el contenedor.

Cómo abrir el complemento de usuarios y equipos de Active Directory

Cómo abrir el complemento Usuarios y equipos de Active Directory:

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

Si no está conectado en el controlador de dominio, debe tener el Administrator Pack de Microsoft correspondiente instalado en el sistema local. Para instalar este Administrator Pack, haga clic en **Inicio**→ **Ejecutar**, escriba MMC y oprima <Entrar>.

Aparecerá la ventana Consola de administración de Microsoft (MMC).

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).
3. Haga clic en **Agregar o quitar complemento**.
4. Seleccione el complemento **Usuarios y equipos de Active Directory** y haga clic en **Agregar**.
5. Haga clic en **Cerrar** y haga clic en **Aceptar**.

Cómo agregar usuarios y privilegios del CMC a Active Directory

El complemento Usuarios y equipos de Active Directory ampliado por Dell le permite agregar usuarios y privilegios del CMC mediante la creación de objetos de RAC, de asociación y de privilegio. Para agregar cada tipo de objeto deberá:

1. Cree un objeto de dispositivo de RAC.
2. Cree un objeto de privilegio.
3. Cree un objeto de asociación.
4. Agregue los objetos a un objeto de asociación.

Creación de un objeto de dispositivo de RAC

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Aparece la ventana **Nuevo objeto**.
3. **Escriba un nombre para el nuevo objeto**. El nombre debe ser idéntico al nombre del CMC que usted va a introducir en el paso 8a de [Configuración del CMC con Active Directory de esquema ampliado y la interfaz web](#).
4. Seleccione **Objeto de dispositivo de RAC**.
5. Haga clic en **OK (Aceptar)**.

Creación de un objeto de privilegio

 **NOTA:** Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Aparece la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
7. Haga clic en la ficha **Privilegios del RAC** y seleccione los privilegios que desea otorgar al usuario. Para obtener más información sobre los privilegios de usuarios del CMC, consulte [Tipos de usuarios](#).

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El ámbito de la asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Cuando cree un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objeto que quiere agregar.

Por ejemplo, si selecciona **Universal** los objetos de asociación sólo estarán disponibles cuando el dominio de Active Directory funcione en el modo nativo o superior.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Esto abrirá la ventana **Nuevo objeto**.
3. Escriba un nombre para el nuevo objeto.

4. Seleccione **Objeto de asociación**.
5. Seleccione el ámbito para el **objeto de asociación**.
6. Haga clic en **OK (Aceptar)**.

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades de objeto de asociación**, puede asociar a usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta Windows 2000 o posteriores, utilice los grupos universales para abarcar dominios con los objetos de RAC o usuario.

Puede agregar a grupos de dispositivos de RAC y usuarios. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

1. Haga clic con el botón derecho del mouse en el **objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Escriba el nombre de grupo de usuarios o usuario y haga clic en **Aceptar**.

Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentican en un dispositivo RAC. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

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

Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados con la red que están disponibles para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de RAC a un objeto de asociación.

Cómo agregar dispositivos de RAC o grupos de dispositivos de RAC

Para agregar dispositivos de RAC o grupos de dispositivos de RAC:

1. Seleccione la ficha **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 en **Aceptar**.

Configuración del CMC con Active Directory de esquema ampliado y la interfaz web

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Red/Seguridad**, y luego haga clic en la subficha **Active Directory**. Aparecerá la página **Menú principal de Active Directory**.
4. Seleccione el botón de radio **Configurar** y luego haga clic en **Siguiente**. Aparecerá la página **Configuración y administración de Active Directory**.
5. En la sección **Valores comunes**:
 - a. Seleccione la casilla **Activar Active Directory** para que quede marcada.
 - b. Escriba el **nombre del dominio raíz**. El **nombre del dominio raíz** es el nombre del dominio raíz completamente calificado para el bosque.

 **NOTA:** El **Nombre del dominio raíz** debe ser un nombre de dominio válido expresado mediante la convención *x.y*, donde *x* es una cadena ASCII de 1 a 256 caracteres sin espacios intermedios, e *y* es un tipo de dominio válido como *com*, *edu*, *gov*, *int*, *mil*, *net* u *org*.

- c. Escriba el **Tiempo de espera** en segundos. **Rango de configuración:** de 15 a 300 segundos. **Valor predeterminado:** 90 segundos
6. **Opcional:** si desea que la llamada dirigida realice una búsqueda en el controlador de dominio y el catálogo global, seleccione la casilla **Buscar servidor de AD para buscar (opcional)** y después:
- En el campo de texto **Controlador de dominio**, escriba el servidor en el que está instalado el servicio Active Directory.
 - En el campo de texto **Catálogo global**, escriba la ubicación del catálogo global en el controlador de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory.
7. Seleccione el botón de radio **Usar esquema ampliado** de la sección **Selección del esquema de Active Directory**.
8. En la sección **Configuración del esquema ampliado:**
- Escriba el **Nombre del CMC**. El **Nombre del CMC** identifica de forma exclusiva la tarjeta del CMC en Active Directory. El **Nombre del CMC** debe ser igual al nombre común del nuevo objeto de CMC que creó en el controlador de dominio. El **Nombre del CMC** debe ser una cadena ASCII de 1 a 256 caracteres sin espacios intermedios.
 - Escriba el **Nombre de dominio del CMC** (ejemplo: `cmc.com`). El **Nombre de dominio del CMC** es el nombre DNS (cadena de caracteres) del dominio donde reside el objeto CMC de Active Directory. El nombre debe ser un nombre de dominio válido que consista en *x.y*, donde *x* es una cadena de 1 a 256 caracteres ASCII sin espacios entre ellos, y *y* es un tipo de dominio válido, como `com`, `edu`, `gov`, `int`, `mil`, `net` u `org`.
9. Haga clic en **Aplicar** para guardar la configuración.
-  **NOTA:** Antes de continuar en el paso siguiente, que permite acceder a otra página, debe aplicar los valores de configuración. De lo contrario, la configuración que ingresó se perderá cuando acceda a esta nueva página.
10. Haga clic en **Volver al menú principal de Active Directory**.
11. Seleccione el botón de radio **Cargar certificado de AD** y haga clic en **Siguiente**. Aparecerá la página **Carga del certificado**.
12. Escriba la ruta del archivo del certificado en el campo de texto o haga clic en **Examinar** para seleccionar el archivo del certificado.
-  **NOTA:** El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.
- Los certificados SSL para el controlador de dominio deben estar firmados por la autoridad de certificados raíz. El certificado con la firma de la autoridad de certificados raíz debe estar disponible en la estación de administración que tiene acceso al CMC.
13. Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
14. Vuelva a iniciar sesión en la interfaz web del CMC.
15. En el árbol del sistema, seleccione **Chasis**, haga clic en la ficha **Red/Seguridad** y luego en la subficha **Red**. Aparecerá la página **Configuración de la red**.
16. Si la casilla **Usar DHCP (para la dirección IP del NIC)** se encuentra activada (seleccionada), realice una de las siguientes operaciones:
- Seleccione la opción **Use el DHCP para obtener direcciones de servidor DNS** para que el servidor DHCP obtenga automáticamente las direcciones del servidor DNS, o bien
 - Configure manualmente una dirección IP de servidor DNS: deseleccione la casilla **Usar DHCP para obtener direcciones de servidor DNS** y luego escriba la dirección IP principal y alternativa del servidor DNS en los campos correspondientes.
17. Haga clic en **Aplicar cambios**.

Ha concluido la configuración de componente Active Directory de esquema ampliado del CMC.

Configuración del CMC con Active Directory de esquema ampliado y RACADM

Los siguientes comandos permiten configurar el componente Active Directory del CMC con esquema ampliado por medio de la herramienta de CLI de RACADM en lugar de utilizar la interfaz web.

- Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

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

racadm config -g cfgActiveDirectory -o cfgADType 1

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

racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre completo del dominio raíz>

racadm config -g cfgActiveDirectory -o cfgADRacName <nombre común del CMC>

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

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del CMC>
```

Opcional: si desea especificar un servidor de catálogo global o LDAP en lugar de utilizar los servidores ofrecidos por el servidor DNS para buscar un nombre de usuario, escriba el siguiente comando para activar la opción **Especificar servidor**:

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

NOTA: Cuando se utiliza la opción **Especificar servidor**, el nombre del host del certificado firmado por una autoridad de certificados no se compara con el nombre del servidor especificado. Esto resulta especialmente útil para los administradores del CMC porque permite ingresar un nombre de host además de una dirección IP.

Después de activar la opción **Especificar servidor**, puede especificar un servidor LDAP y un catálogo global con direcciones IP o nombres completos de dominios (FQDN) de los servidores. Los nombres FQDN consisten en los nombres de host y de dominio de los servidores.

Para especificar un servidor de LDAP, escriba:

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <dirección IP de controlador de dominio AD>
```

Para especificar un servidor de catálogo global, escriba:

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <dirección IP de catálogo global>
```

NOTA: Si la dirección IP se define con el valor 0.0.0.0, el CMC no podrá buscar un servidor.

NOTA: Puede especificar una lista de servidores de LDAP o de catálogo global separados por comas. El CMC permite especificar hasta tres direcciones IP o nombres de host.

NOTA: Si los servidores LDAP no se configuran correctamente para todos los dominios y las aplicaciones, pueden producirse resultados inesperados durante el funcionamiento de las aplicaciones y los dominios existentes.

2. Especifique un servidor DNS por medio de una de las siguientes opciones:

- 1 Si DHCP está activado en el CMC y desea utilizar la dirección de DNS obtenida automáticamente por el servidor DHCP, escriba el siguiente comando:

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

- 1 Si DHCP no está activado en el CMC o está activado pero desea especificar la dirección IP de DNS de forma manual, escriba los siguientes comandos:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

De esta forma quedará configurada la función de esquema ampliado.

Generalidades del esquema estándar de Active Directory

El uso del esquema estándar para integrar Active Directory requiere tareas de configuración en Active Directory y el CMC.

En Active Directory, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso al CMC será miembro del grupo de funciones.

Para que este usuario tenga acceso a una tarjeta de CMC específica, es necesario configurar el nombre del grupo de funciones y su dominio en dicha tarjeta de CMC. A diferencia del esquema ampliado, en este caso la función y el nivel de privilegios se definen en cada tarjeta de CMC y no en Active Directory. En cada CMC pueden configurarse y definirse hasta cinco grupos de funciones. La [tabla 5-10](#) muestra el nivel de privilegios de los grupos de funciones y la [tabla 7-8](#) muestra la configuración predeterminada del grupo de funciones.

Figura 7-4. Configuración del CMC con Active Directory y esquema estándar

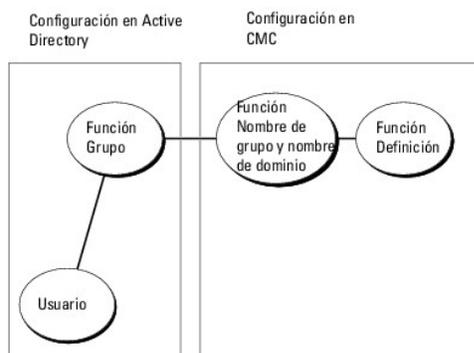


Tabla 7-8. Privilegios predeterminados del grupo de funciones

Grupo de funciones	Privilegio predeterminado Nivel	Permisos concedidos	Máscara de bits
1	Ninguno	<ul style="list-style-type: none"> Usuario con acceso al CMC Administrador de configuración del chasis Administrador de configuración de usuarios Administrador de borrado de registros Administrador de control del chasis (comandos avanzados) Super usuario Server Administrator Usuario de alertas de prueba Usuario de comando de depuración de errores Administrador de estructura de red A Administrador de estructura de red B Administrador de estructura de red C 	0x00000fff
2	Ninguno	<ul style="list-style-type: none"> Usuario con acceso al CMC Administrador de borrado de registros Administrador de control del chasis (comandos avanzados) Server Administrator Usuario de alertas de prueba Administrador de estructura de red A Administrador de estructura de red B Administrador de estructura de red C 	0x000000f9
3	Ninguno	Usuario con acceso al CMC	0x00000001
4	Ninguno	Sin permisos asignados	0x00000000
5	Ninguno	Sin permisos asignados	0x00000000

 **NOTA:** Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

 **NOTA:** Para obtener más información sobre los privilegios de usuarios, consulte [Tipos de usuarios](#).

Hay dos maneras de activar el esquema estándar de Active Directory:

1. Por medio de la interfaz web del CMC. Consulte el apartado [Configuración del CMC con Active Directory de esquema estándar y la interfaz web](#).
1. Con la herramienta de CLI de RACADM. Consulte el apartado [Configuración del CMC con Active Directory de esquema estándar y RACADM](#).

Configuración de Active Directory de esquema estándar para acceder al CMC

Para que un usuario pueda acceder al CMC, en primer lugar es necesario ejecutar los pasos que se indican a continuación para configurar Active Directory:

1. En un servidor de Active Directory (controlador de dominio), abra el complemento de usuarios y equipos de Active Directory.
2. Cree un grupo o seleccione un grupo existente. El nombre del grupo y el nombre de este dominio deberán configurarse en el CMC por medio de la interfaz web o de RACADM.

Para obtener más información, consulte [Configuración del CMC con Active Directory de esquema estándar y la interfaz web](#) o [Configuración del CMC con Active Directory de esquema estándar y RACADM](#).

3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al CMC.

Configuración del CMC con Active Directory de esquema estándar y la interfaz web

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Red/Seguridad**, y luego haga clic en la subficha **Active Directory**. Aparecerá la página **Menú principal de Active Directory**.
4. Seleccione la opción **Configurar** y haga clic en **Siguiente**. Aparecerá la página **Configuración y administración de Active Directory**.
5. En la sección **Valores comunes**:
 - a. Seleccione la casilla de marcación **Activar Active Directory**.
 - b. Escriba el **Nombre del dominio raíz**. El **nombre del dominio RAÍZ** es el nombre del dominio raíz completamente calificado para el bosque.

 **NOTA:** El **Nombre del dominio RAÍZ** debe ser un nombre de dominio válido expresado mediante la convención x.y, donde x es una cadena ASCII de 1 a 256 caracteres sin espacios intermedios, e y es un tipo de dominio válido como com, edu, gov, int, mil, net u org.

- c. Escriba el **Tiempo de espera** en segundos. **Rango de configuración:** de 15 a 300 segundos. **Valor predeterminado:** 90 segundos
6. **Opcional:** si desea que la llamada dirigida realice una búsqueda en el controlador de dominio y el catálogo global, seleccione la casilla **Buscar servidor de AD para buscar (opcional)** y después:
 - a. En el campo de texto **Controlador de dominio**, escriba el servidor en el que está instalado el servicio Active Directory.
 - b. En el campo de texto **Catálogo global**, escriba la ubicación del catálogo global en el controlador de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory.
7. Haga clic en **Utilizar esquema estándar** en la sección Selección del esquema de Active Directory.
8. Haga clic en **Aplicar** para guardar la configuración.

 **NOTA:** Antes de continuar en el paso siguiente, que permite acceder a otra página, debe aplicar los valores de configuración. De lo contrario, la configuración que ingresó se perderá cuando acceda a esta nueva página.

9. En la sección **Configuración del esquema estándar**, haga clic en un **Grupo de funciones**. Aparecerá la página **Configurar grupo de funciones**.
10. Escriba el **Nombre de grupo**. El nombre de grupo identifica el grupo de funciones en el servicio Active Directory relacionado con la tarjeta del CMC.
11. Escriba el **Dominio de grupo**. El **Nombre de grupo** es el nombre completo del dominio raíz para el bosque.
12. En la página **Privilegios del grupo de funciones**, seleccione los privilegios del grupo.

Si modifica alguno de los privilegios, el **privilegio del grupo de funciones** ya existente (**administrador**, **usuario avanzado** o **usuario invitado**) cambiará al grupo personalizado o el privilegio de grupo de funciones que corresponda. Consulte el apartado [tabla 5-10](#).

13. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.
14. Haga clic en **Volver a la configuración y administración de Active Directory**.
15. Haga clic en **Volver al menú principal de Active Directory**.
16. Cargue el certificado raíz de bosque de dominio firmado por una autoridad de certificados en el CMC.
 - a. Seleccione la casilla de marcación **Cargar certificado de CA de Active Directory** y después haga clic en **Siguiente**.
 - b. En la página **Carga del certificado**, escriba la ruta de acceso del archivo del certificado o desplácese al directorio del archivo del certificado.

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

Los certificados SSL para los controladores de dominio deben estar firmados con el certificado de firma autorizada por la autoridad de certificados raíz. El certificado con la firma de la autoridad de certificados raíz debe estar disponible en la estación de administración que tiene acceso al CMC.

- c. Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
17. Cierre sesión y luego inicie sesión en el CMC para completar la configuración del componente Active Directory del CMC.
18. Seleccione **Chasis** en el árbol del sistema.
19. Haga clic en la ficha **Red/Seguridad**.
20. Haga clic en la subficha **Red**. Aparecerá la página **Configuración de la red**.
21. Si **Usar DHCP (para la dirección IP del NIC)** está seleccionado en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

Para introducir manualmente una dirección IP del servidor DNS, deselectione **Usar DHCP para obtener las direcciones del servidor DNS** y escriba las direcciones IP principal y alternativa del servidor DNS.

22. Haga clic en **Aplicar cambios**.

De esta forma quedará configurada la función de Active Directory de esquema estándar para el CMC.

Configuración del CMC con Active Directory de esquema estándar y RACADM

Para configurar el componente Active Directory del CMC con esquema estándar por medio de la CLI de RACADM, utilice los siguientes comandos:

1. Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

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

```

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRootDomain <nombre completo del dominio raiz>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupName <nombre común del grupo de funciones>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupDomain <nombre completo de dominio>

racadm config -g cfgStandardSchema -i <indice> -o cfgSSADRoleGroupPrivilege <número de máscara de bits para permisos de usuario específicos>

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

racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>

```

 **NOTA:** Para obtener los valores del número de máscara de bits, consulte [Máscaras de bit para privilegios del usuario](#).

2. Especifique un servidor DNS por medio de una de las siguientes opciones:

- 1 Si DHCP está activado en el CMC y desea utilizar la dirección de DNS obtenida automáticamente por el servidor DHCP, escriba el siguiente comando:

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

- 1 Si DHCP está deshabilitado en el CMC o desea introducir manualmente la dirección IP de DNS, escriba los siguientes comandos:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección IP principal de DNS>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP secundaria de DNS>
```

Preguntas más frecuentes

[Tabla 7-9](#) ofrece una lista de las preguntas más frecuentes sobre el uso de Active Directory con el CMC y sus respuestas.

Tabla 7-9. Uso del CMC con Active Directory: Preguntas frecuentes

Pregunta	Respuesta
¿Puedo iniciar sesión en el CMC mediante el uso de Active Directory en varios árboles?	Sí El algoritmo de consulta de Active Directory del CMC admite varios árboles en un sólo bosque.
¿El inicio de sesión en el CMC mediante Active Directory funciona en el modo mixto (es decir, los controladores de dominio en el bosque ejecutan diferentes sistemas operativos, como Microsoft Windows® 2000 o Windows Server® 2003)?	Sí En el modo mixto, todos los objetos utilizados por el proceso de consulta del CMC (entre el usuario, el objeto de dispositivo del RAC y el objeto de asociación) tienen que estar en el mismo dominio. El complemento 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 CMC con Active Directory admite varios entornos de dominio?	Sí El nivel de función del bosque de dominio debe estar en modo Nativo o en modo de Windows 2003. Además, los grupos entre objeto de asociación, objetos de usuario de RAC, y objetos de dispositivo de RAC (incluso el objeto de asociación) deben ser grupos universales.
¿Estos objetos ampliados por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?	El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento Usuarios y equipos de Active Directory ampliado por Dell obliga a crear estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes.
¿Hay alguna restricción para la configuración del controlador de dominio de SSL?	Sí Todos los certificados SSL para los servidores Active Directory que se encuentran en el bosque deben estar firmados mediante el mismo certificado con firma de la autoridad de certificados raíz, pues el CMC sólo permite cargar un certificado SSL firmado por una autoridad de certificados de confianza.
Creé y cargué un nuevo certificado de RAC y ahora la interfaz web no se inicia.	Si utiliza los servicios de certificados de Microsoft para generar el certificado de RAC, existe la posibilidad de que inadvertidamente haya seleccionado la opción Certificado de usuario en lugar de Certificado de web cuando creó el certificado. Para resolver el problema, genere una CSR y luego cree un nuevo certificado de web por medio de los servicios de certificados de Microsoft y después cárguelo mediante los siguientes comandos de RACADM: racadm sslsrngen [-g] [-u] [-f { nombre de archivo }] racadm sslcertupload -t 1 -f {web_sslcert}
¿Qué debo hacer si no puedo iniciar sesión en el CMC mediante la autenticación de Active Directory? ¿Cómo soluciono el problema?	<ol style="list-style-type: none"> 1. Asegúrese de usar el nombre de dominio de usuario correcto durante un inicio de sesión y no el nombre de NetBIOS. 2. Si posee una cuenta de usuario del CMC local, inicie sesión en el CMC por medio

de sus credenciales locales.

Después de que haber iniciado sesión, realice los pasos a continuación:

- a. Asegúrese de haber seleccionado la casilla **Habilitar Active Directory** en la página de configuración de Active Directory del CMC.
- b. En la página de configuración de red del CMC, asegúrese que la configuración de DNS sea correcta.
- c. Asegúrese de haber cargado en el CMC el certificado de Active Directory desde el certificado con firma 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 lo datos de las opciones **Nombre del CMC**, **Nombre del dominio raíz** y **Nombre de dominio del CMC** coincidan con la configuración del entorno de Active Directory.
- f. Verifique que la contraseña del CMC tenga 127 caracteres como máximo. Si bien el CMC admite contraseñas de hasta 256 caracteres, en Active Directory las contraseñas sólo pueden tener 127 caracteres como máximo.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Definiciones de grupos y objetos de bases de datos de propiedades del CMC

Guía del usuario

- [Caracteres que se pueden mostrar](#)
- [idRacInfo \(sólo lectura\)](#)
- [cfgLanNetworking](#)
- [cfgCurrentLanNetworking \(sólo lectura\)](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgNetTuning](#)
- [cfgOobSntp](#)
- [cfgTraps](#)
- [cfgAlerting](#)
- [cfgRacTuning](#)
- [cfgRacSecurity](#)
- [cfgActiveDirectory](#)
- [cfgStandardSchema](#)
- [cfgChassisPower](#)
- [cfgServerInfo](#)
- [cfgKVMInfo](#)

La base de datos de propiedades del CMC contiene la información de configuración del CMC. 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.

Utilice las identificaciones de objetos y grupos con los subcomandos de RACADM **config** (consulte [config](#)) y **getconfig** (consulte [getconfig](#)) para configurar el CMC. Las secciones siguientes describen cada objeto e indican si el objeto se puede leer, escribir, o ambos.

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

idRacInfo (sólo lectura)

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Usuario con acceso al CMC**.

Descripción

Muestra información de las propiedades del CMC. **Es de sólo lectura.**

Sinopsis

```
racadm getconfig -g idRacInfo
```

#idRacType

Identifica el tipo de controlador de acceso remoto como el CMC.

#idRacProductInfo

Utiliza una cadena de texto para identificar el producto; por ejemplo, Chassis Management Controller.

#idRacDescriptionInfo

Una descripción de texto del tipo de RAC.

#idRacVersionInfo

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

#idRacBuildInfo

La versión actual de la compilación de software del RAC.

#idRacName

Nombre asignado por un usuario que identifica al CMC.

Ejemplo

```
racadm getconfig -g idRacInfo

# idRacType=8
# idRacProductInfo=Chassis Management Controller
# idRacDescriptionInfo=This system component provides a complete set of remote management functions for blade servers
# idRacVersionInfo=P21
# idRacBuildInfo=200708301525
# idRacName=CMC-1
```

cfgLanNetworking

-  **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.
-  **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.
-  **NOTA:** Puede configurarse cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Muestra información sobre las propiedades relacionadas con la red y permite configurarlas.

Sinopsis

```
racadm getconfig -g cfgLanNetworking
```

cfgNicEnable

Activa o desactiva la tarjeta de interfaz de red del CMC. Si esta propiedad se configura con el valor 0 (falso), no será posible acceder a las interfaces de red remota con el CMC, que sólo estará disponible a través de las interfaces serie de RACADM.

- 1 **Opciones de configuración:** 1 (verdadero), 0 (falso)
- 1 **Valor predeterminado:** 1

cfgNicIpAddress

Asigna una dirección IP estática al CMC. Esta propiedad sólo se utiliza si **cfgNicUseDhcp** se define con el valor 0 (falso).

- 1 **Valor legal:** una cadena de caracteres que represente una dirección IP válida. Por ejemplo, 192.168.0.20.

cfgNicNetmask

Asigna una máscara de subred estática para la dirección IP del CMC. Esta propiedad sólo se utiliza si **cfgNicUseDhcp** se define con el valor 0 (falso).

- 1 **Valor legal:** una cadena de caracteres que represente una máscara de subred válida. Por ejemplo: 255.255.255.0.

cfgNicGateway

Asigna una puerta de enlace estática para la dirección IP del CMC. Esta propiedad sólo se utiliza si **cfgNicUseDhcp** se define con el valor 0 (falso).

- 1 **Valor legal:** una cadena de caracteres que represente una puerta de enlace válida. Por ejemplo, 192.168.0.1.

cfgNicUseDhcp

Activa o desactiva el uso de DHCP (Protocolo de configuración dinámica de host) por parte del CMC para el NIC. Si está establecido en 0, el DHCP está desactivado y las direcciones IP se asignan de forma estática. Si está establecido en 1, el DHCP está activado y las direcciones IP se asignan automáticamente.

- 1 **Opciones de configuración:** 1 (verdadero), 0 (falso)
- 1 **Valor predeterminado:** 0

#cfgNicMacAddress

Es de sólo lectura. Dirección MAC del CMC; formato: dd:dd:dd:dd:dd:dd, donde **d** es un dígito hexadecimal en el rango 0 - 9, A - F

cfgDNSServersFromDHCP (lectura/escritura)

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

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

- 1 **Opciones de configuración:** 1 (verdadero), 0 (falso)
- 1 **Valor predeterminado:** 0

cfgDNSServer1 (lectura/escritura)

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

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

- 1 **Opciones de configuración:** una cadena que representa una dirección IP válida, por ejemplo: 192.168.0.20.

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

cfgDNSServer2 (lectura/escritura)

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

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

- 1 **Opciones de configuración:** una cadena que representa una dirección IP válida, por ejemplo: 192.168.0.20.
- 1 **Valor predeterminado:** 0.0.0.0

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

cfgDNSRacName

Muestra el nombre del CMC. Este parámetro sólo se usa cuando **cfgDNSRegisterRac** se define con el valor 1 (verdadero).

- 1 **Opciones de configuración:** una cadena de hasta 63 caracteres alfanuméricos y guiones que debe comenzar con una letra. Por ejemplo: `cmc-1, d-345`.
- 1 **Valor predeterminado:** `cmc-<etiqueta de servicio>`

cfgDNSDomainName

Muestra el nombre del dominio DNS. Este parámetro sólo aparece cuando `cfgDNSDomainNameFromDHCP` se define con el valor 0 (falso).

- 1 **Opciones de configuración:** cadena de hasta 254 caracteres alfanuméricos y guiones *que debe comenzar con una letra*. Ejemplo: `p45, a-tz-1, rid-`.
- 1 **Valor predeterminado:** ""

cfgDNSDomainNameFromDHCP

Especifica si el nombre del dominio DNS del CMC es asignado por el servidor DHCP de red.

- 1 **Opciones de configuración:** 1 (verdadero), 0 (falso)
- 1 **Valor predeterminado:** 0

cfgDNSRegisterRac

Registra el nombre del CMC en el servidor DNS.

- 1 **Opciones de configuración:** 1 (verdadero), 0 (falso)
- 1 **Valor predeterminado:** 0

Ejemplo

```
racadm getconfig -g cfgLanNetworking
```

```
cfgNicEnable=1
cfgNicIpAddress=192.168.22.101
cfgNicNetmask=255.255.255.0
cfgNicGateway=192.168.22.101
cfgNicUseDhcp=1
#cfgNicMacAddress=00:00:00:00:00:01
cfgDNSServersFromDHCP=0
cfgDNSServer1=192.168.0.5
cfgDNSServer2=192.168.0.6
cfgDNSRacName=d-345
cfgDNSDomainName=d-
cfgDNSDomainNameFromDHCP=0
cfgDNSRegisterRac=0
```

cfgCurrentLanNetworking (sólo lectura)

 **NOTA:** Utilice este objeto con el subcomando `getconfig`.

Descripción

Muestra las propiedades actuales de la tarjeta de interfaz de red del CMC.

Sinopsis

```
racadm getconfig [-g] [-o <nombre de objeto>] [-h] cfgCurrentLanNetworking
```

```
racadm config [-g] [-o <nombre de objeto>] [-h] cfgCurrentLanNetworking
```

cfgNicCurrentIpAddress

Muestra la dirección IP estática del CMC.

cfgNicCurrentNetmask

Muestra la máscara de subred estática de la dirección IP del CMC.

cfgNicCurrentGateway

Muestra la puerta de enlace estática de la dirección IP del CMC.

cfgNicCurrentDhcpWasUsed

Indica si se utiliza DHCP para configurar la tarjeta de interfaz de red:

1: la dirección es estática.

0: la dirección se obtuvo del servidor DHCP.

cfgDNSCurrentServer1

Muestra la dirección IP del servidor DNS 1.

cfgDNSCurrentServer2

Muestra la dirección IP del servidor DNS 2.

cfgDNSCurrentDomainName

Muestra el nombre del dominio DNS.

Ejemplo

```
racadm getconfig -g cfgCurrentLanNetworking

# cfgNicCurrentIpAddress=143.166.152.116
# cfgNicCurrentNetmask=255.255.255.0
# cfgNicCurrentGateway=143.166.152.1
# cfgNicCurrentDhcpWasUsed=0
# cfgDNSCurrentServer1=192.168.0.5
# cfgDNSCurrentServer2=192.168.0.6
# cfgDNSCurrentDomainName=MYDOMAIN
```

cfgRemoteHosts

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Activa o desactiva y configura las actualizaciones de firmware y alertas por correo electrónico de SMTP.

cfgRhostsFwUpdateTftpEnable

Activa o desactiva las actualizaciones de firmware del CMC desde un servidor TFTP de red.

1 **Opciones de configuración:** 1 (verdadero), 0 (falso)

1 **Valor predeterminado:** 1

cfgRhostsFwUpdateIpAddr

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

Opciones de configuración: cadena de caracteres que represente una dirección IP de servidor SMTP válida. Por ejemplo: 192.168.0.55.

Valor predeterminado: 0.0.0.0

cfgRhostsFwUpdatePath

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

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

Valor legal: cadena de hasta 255 caracteres.

cfgRhostsSmtServerIpAddr

Especifica la dirección IP del servidor SMTP de red, que transmite alertas de correo electrónico desde el CMC si las alertas están configuradas y activadas.

Valor legal: cadena de caracteres que represente una dirección IP de servidor TFTP válida. Por ejemplo: 192.168.0.55.

Valor predeterminado: 0.0.0.0

Ejemplo

```
racadm getconfig -g cfgRemoteHosts

cfgRhostsFwUpdateTftpEnable=1
cfgRhostsFwUpdateIpAddr=127.0.0.1
cfgRhostsFwUpdatePath=m13_0417.bin
cfgRhostsSmtServerIpAddr=localhost.localdomain
```

cfgUserAdmin

 **NOTA:** En la versión del firmware del CMC actual, los objetos `cfgUserAdminEnable` y `cfgUserAdminPrivilege` están interrelacionados y si se modifica el valor de una propiedad también se modificará el valor de la otra. Por ejemplo, si un usuario no tiene privilegios de inicio de sesión, estará deshabilitado de forma predeterminada. Si para activar el usuario se modifica el valor de `UserAdminEnable` para que sea 1, el dígito que se encuentra en el extremo derecho de `UserAdminPrivilege` también pasará a ser 1. Por otra parte, si se modifica el valor del dígito situado en el extremo derecho de `UserAdminPrivilege` para que sea 0, el valor de `UserAdminEnable` también pasará a ser 0.

 **NOTA:** Utilice este objeto con los subcomandos `config` o `getconfig`. Debe suministrar un número de grupo de índices para usar estos comandos de la siguiente manera: **-i <grupo de índices>**

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción `-o`.

Descripción

Muestra información de los usuarios del CMC y permite configurarlos.

cfgUserAdminIndex

Es de sólo lectura. Muestra el número de índice. El número de índice se utiliza para especificar un nombre de grupo único. Sólo es válido para los grupos indexados. El índice se especifica con un número entero decimal de 1 a 6.

cfgUserAdminEnable

Activa o desactiva un usuario individual.

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgUserAdminUserName

Muestra y define el nombre del usuario correspondiente al nombre de índice especificado. 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 dos comillas (") se elimina al usuario de ese índice. Para cambiar el nombre, es necesario eliminarlo y volver a crearlo. La cadena no puede contener "/" (diagonal), "\" (diagonal invertida), "." (punto), "@" (arroba) ni comillas.

Valor legal: cadena de hasta 16 caracteres.

cfgUserAdminPassword

Es de sólo escritura. Muestra la contraseña correspondiente al índice de este usuario en forma de serie de asteriscos (*). Una vez que se define la propiedad, no puede visualizarse.

cfgUserAdminPrivilege

Especifica los privilegios de autoridad basada en funciones para el usuario. El valor se representa como una máscara de bits que permite definir cualquier combinación de valores de privilegios. [Tabla B-1](#) describe las máscaras de bit permitidas. [Tabla B-2](#) proporciona ejemplos de las máscaras de bit de privilegios para usuarios con uno o más privilegios.

Opciones de configuración: 0x0000000-0x0000fff, and 0x0

Valor predeterminado: 0x0000000

Ejemplo

```
racadm getconfig -g cfgUserAdmin -i 1

# cfgUserAdminIndex=1
cfgUserAdminEnable=1
cfgUserAdminUserName=root
# cfgUserAdminPassword=***** (Write-Only)
cfgUserAdminPrivilege=0x00000fff
```

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

Privilegio del usuario	Máscara de bits de privilegios
Usuario con acceso al CMC	0x0000001
Administrador de configuración del chasis	0x0000002
Administrador de configuración de usuarios	0x0000004
Administrador de borrado de registros	0x0000008
Administrador de control del chasis	0x0000010
Super usuario	0x0000020
Server Administrator	0x0000040
Usuario de alertas de prueba	0x0000080
Administrador de comandos de depuración de errores	0x0000100
Administrador de estructura de red A	0x0000200
Administrador de estructura de red B	0x0000400
Administrador de estructura de red C	0x0000800

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

Privilegio del usuario	Máscara de bits de privilegios
El usuario no tiene permiso para acceder al CMC.	0x00000000
El usuario sólo puede iniciar sesión en el CMC y visualizar información sobre la configuración del servidor y el CMC.	0x00000001
El usuario puede iniciar sesión y configurar el CMC.	0x00000001 + 0x00000002 = 0x00000003

cfgEmailAlert

 **NOTA:** Utilice este objeto con los subcomandos `config` o `getconfig`.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción -o.

Descripción

Configura las alertas por correo electrónico del CMC.

cfgEmailAlertIndex

Es de sólo lectura. Muestra el índice único de una alerta.

Rango de configuración: de 1 a 4

Valor predeterminado: este parámetro se determina en función de las instancias existentes.

cfgEmailAlertEnable

Activa o desactiva las alertas por correo electrónico del CMC.

Opciones de configuración: 1 (activar), 0 (desactivar)

Valor predeterminado: 0 (desactivado)

cfgEmailAlertAddress

Es de sólo lectura. Indica la dirección de correo electrónico de destino para las alertas por correo electrónico.

Opciones de configuración: formato de dirección de correo electrónico con un máximo de 64 caracteres ASCII.

Valor predeterminado: [nulo]

cfgEmailAlertEmailName

Especifica el nombre u otro identificador relacionado con la dirección de correo electrónico de destino. El nombre de correo electrónico puede hacer referencia a un individuo, grupo, ubicación, departamento, etc.

Opciones de configuración: cadena de hasta 32 caracteres.

Valor predeterminado: [nulo]

Ejemplo

```
racadm getconfig -g cfgEmailAlert -i 2
```

```
# cfgEmailAlertIndex=1
cfgEmailAlertEnable=1
cfgEmailAlertAddress=kfulton@dell.com
cfgEmailAlertName=Kevin Fulton
```

cfgSessionManagement

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Define y muestra la configuración actual de las propiedades de tiempo de espera en inactividad de las sesiones del servidor web, Telnet, SSH y RACADM. Los cambios en la configuración de tiempo de espera en inactividad se aplicarán en la siguiente sesión. Para desactivar el tiempo de espera en inactividad para una conexión, defina esta propiedad en 0.

Objetos

cfgSsnMgtWebserverTimeout

Especifica la cantidad de segundos que deben transcurrir antes de que una conexión inactiva con el servidor web finalice automáticamente.

Rango de configuración: de 60 a 1920 segundos.

Valor predeterminado: 300 segundos

cfgSsnMgtTelnetIdleTimeout

Especifica la cantidad de segundos que deben transcurrir antes de que una sesión de Telnet inactiva finalice automáticamente.

Opciones de configuración: 0 (sin tiempo de espera); 60-1920 segundos

Valor predeterminado: 300 segundos

cfgSsnMgtSshIdleTimeout

Especifica la cantidad de segundos que deben transcurrir antes de que una sesión Secure Shell inactiva finalice automáticamente.

Opciones de configuración: 0 (sin tiempo de espera); 60-1920 segundos

Valor predeterminado: 300 segundos

cfgSsnMgtRacadmTimeout

Especifica la cantidad de segundos que deben transcurrir antes de que una conexión de RACADM remota que está inactiva finalice automáticamente.

Rango de configuración: de 10 a 1920 segundos.

Valor predeterminado: 30 segundos

Ejemplo

```
racadm getconfig -g cfgSessionManagement
```

```
cfgSsnMgtWebserverTimeout=0  
cfgSsnMgtTelnetIdleTimeout=0  
cfgSsnMgtSshIdleTimeout=300  
cfgSsnMgtRacadmTimeout=0
```

cfgSerial

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Muestra información de los parámetros serie y permite configurarlos.

Objetos

cfgSerialBaudRate

Establece la velocidad en baudios en el puerto serie del CMC.

Opciones de configuración: 9600, 19200, 28800, 38400, 57600, 115200

Valor predeterminado: 115200

cfgSerialConsoleEnable

Activa o desactiva la interfaz de consola serie del CMC.

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 1

cfgSerialConsoleQuitKey

Especifica la clave o combinación de claves que da por finalizada la consola de texto serie. El valor puede estar representado por una de las siguientes opciones:

- 1 Valor decimal: por ejemplo, 95
- 1 Valor hexadecimal: por ejemplo, 0x12
- 1 Valor octal: por ejemplo, 007
- 1 Valor ASCII: por ejemplo, <Ctrl>a

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

- a. <Ctrl> con cualquier carácter alfabético (a-z, A-Z)
- b. <Ctrl> con uno de los siguientes caracteres especiales: [] \ ^ _

Valor legal: cadena de hasta 4 caracteres.

Valor predeterminado: <Ctrl><\>

cfgSerialConsoleIdleTimeout

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

Opciones de configuración: 0 (sin tiempo de espera); 60-1920

Valor predeterminado: 300

cfgSerialConsoleNoAuth

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

Opciones de configuración: 0 (activado), 1 (desactivado)

Valor predeterminado: 0

cfgSerialConsoleCommand

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

Ejemplo: "connect server-1"

Valor predeterminado: ""

cfgSerialHistorySize

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

Rango de configuración: de 0 a 8192

Valor predeterminado: 8192

cfgSerialTelnetEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgSerialSshEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 1

Ejemplo

```
racadm getconfig -g cfgSerial
```

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=1920
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand="connect server-1"
cfgSerialHistorySize=1000
cfgSerialTelnetEnable=0
cfgSerialSshEnable=1
```

cfgNetTuning

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Muestra información de los parámetros de ajuste de red del CMC y permite configurarlos.

cfgNetTuningNicSpeed

Especifica la velocidad de la tarjeta de interfaz de red del CMC. Esta propiedad sólo se utiliza si **cfgNetTuningNicAutoNeg** se define con el valor 0 (desactivado).

Opciones de configuración: 10 o 100

Valor predeterminado: 100

cfgNetTuningNicFullDuplex

Especifica la configuración de dúplex de la tarjeta de interfaz de red del CMC. Esta propiedad sólo se utiliza si **cfgNetTuningNicAutoNeg** se define con el valor 0 (desactivado).

Opciones de configuración: 0 (semidúplex), 1 (dúplex completo)

Valor predeterminado: 1

cfgNetTuningNicMtu

Especifica el tamaño en bytes de la unidad de transmisión máxima usada por la tarjeta de interfaz de red del CMC.

Rango de configuración: de 576 a 1500

Valor predeterminado: 1500

cfgNetTuningNicAutoneg

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

Opciones de configuración: 1 (activado), 0 (desactivado)

Valor predeterminado: 1

Ejemplo

```
racadm getconfig -g cfgNetTuning
```

```
cfgNetTuningNicSpeed=100
cfgNetTuningNicFullDuplex=1
cfgNetTuningNicMtu=1500
cfgNetTuningNicAutoneg=1
```

cfgOobSnmpp

-  **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.
-  **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.
-  **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Activa o desactiva y configura las capturas SNMP del CMC.

cfgOobSnmppAgentEnable

Activa o desactiva el agente SNMP en el CMC.

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgOobSnmppAgentCommunity

Define la cadena de comunidad (que es idéntica al nombre de comunidad) utilizada para la autenticación. La cadena de comunidad actúa como una contraseña compartida entre diferentes hosts de la red. Este valor de cadena de comunidad debe coincidir con el de los demás equipos host a fin de que exista cualquier tipo de comunicación por medio de SNMP.

Ejemplo

```
racadm getconfig -g cfgOobSnmpp
```

```
cfgOobSnmppTrapsEnable=1
cfgOobSnmppAgentCommunity=public
```

cfgTraps

-  **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.
-  **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.
-  **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Muestra información y configura el envío de capturas SNMP para un usuario determinado.

cfgTrapsIndex

Es de sólo lectura. Señala el índice único de una instancia de alerta.

cfgTrapsEnable

Activa o desactiva las capturas de sucesos del CMC.

Opciones de configuración: 1 (verdadero), 0 (falso)

cfgTrapsAlertDestIpAddr

Define la dirección IP que recibirá el alerta.

Opciones de configuración: Cadena de caracteres que represente una dirección IP válida. Por ejemplo, 192.168.0.20.

cfgTrapsCommunityName

Define la cadena de comunidad (que es idéntica al nombre de comunidad) utilizada para la autenticación. La cadena de comunidad actúa como una contraseña compartida entre diferentes hosts de la red. Este valor de cadena de comunidad debe coincidir con el de los demás equipos host a fin de que exista cualquier tipo de comunicación por medio de SNMP.

Ejemplo

```
racadm getconfig -g cfgTraps -i 2

# cfgTrapsIndex=2
cfgTrapsEnable=1
cfgTrapsAlertDestIpAddr=
cfgTrapsCommunityName=public
```

cfgAlerting

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Activa o desactiva las alertas de captura de sucesos de SNMP y define el filtro de sucesos.

cfgAlertingEnable

Activa o desactiva las capturas de sucesos del CMC.

Opciones de configuración: 1 (verdadero), 0 (falso)

cfgAlertingFilterMask

Opciones de configuración: Valores hexadecimales 0x0-0x007fffff. Para obtener información sobre los valores hexadecimales, consulte [tabla 11-2](#).

Valor predeterminado: 0x3ff8db

cfgAlertingSourceEmailName

Dirección de correo electrónico que se utiliza para enviar notificaciones por correo electrónico cuando ocurre un suceso.

Ejemplos

```
1 racadm getconfig -g cfgAlerting -o cfgAlertingEnable
0x007fffff
1 racadm config -g cfgAlerting -o cfgAlertingEnable 1

Object value modified successfully.
(El valor del objeto se modificó correctamente.)
```

cfgRacTuning

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getConfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Configura los parámetros de ajustes del CMC.

cfgRacTuneRemoteRacadmEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 1

cfgRacTuneWebserverEnable

Activa y desactiva el servidor web del CMC. Si esta propiedad se define en 0 (FALSO o desactivado), no se podrá acceder al CMC a través de RACADM remoto o exploradores de web cliente. Esta propiedad no tiene ningún efecto en las interfaces Telnet, SSH, serie o RACADM local.

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 1

cfgRacTuneHttpPort

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

Rango de configuración: de 10 a 65535

Valor predeterminado: 80

cfgRacTuneHttpsPort

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

Rango de configuración: de 10 a 65535

Valor predeterminado: 443

cfgRacTuneTelnetPort

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

Rango de configuración: de 10 a 65535

Valor predeterminado: 23

cfgRacTuneSshPort

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

Rango de configuración: de 10 a 65535

Valor predeterminado: 22

cfgRacTuneIpRangeEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgRacTuneIpRangeAddr

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

Opciones de configuración: cadena con formato de dirección IP. Por ejemplo: 192.168.0.44.

Valor predeterminado: 192.168.1.1

cfgRacTuneIpRangeMask

Especifica la propiedad de máscara de rango IP.

Opciones de configuración: valor de máscara de bits aplicado con bits justificados a la izquierda. Por ejemplo: 255.255.255.0.

Valor predeterminado: 255.255.255.0

cfgRacTuneIpBlkEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgRacTuneIpBlkFailCount

Define la cantidad máxima de fallas de inicio de sesión que pueden producirse en la ventana antes de rechazar los intentos de inicio de sesión de la dirección IP.

Rango de configuración: de 2 a 16

Valor predeterminado: 5

cfgRacTuneIpBlkFailWindow

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

Rango de configuración: de 2 a 65535

Valor predeterminado: 60

cfgRacTuneIpBlkPenaltyTime

Define el periodo expresado en segundos en el que se rechazarán las solicitudes de inicio de sesión provenientes de una dirección IP con exceso de fallas.

Rango de configuración: de 2 a 65535

Valor predeterminado: 300

cfgRacTuneTimezoneOffset

Especifica la diferencia expresada en segundos con respecto a la hora universal coordinada (UTC)/hora del meridiano de Greenwich (GMT). Si la zona horaria actual se encuentra al oeste de Greenwich, el valor será negativo.

cfgRacTuneDaylightOffset

Especifica la cantidad de segundos de horario de verano incluidos en la zona horaria actual. Si la zona horaria no corresponde al horario de verano, el valor será 0.

Ejemplo

```
racadm getconfig -g cfgRacTuning
```

```
cfgRacTuneRemoteRacadmEnable=1
cfgRacTuneWebserverEnable=1
cfgRacTuneHttpPort=80
cfgRacTuneHttpsPort=443
cfgRacTuneTelnetPort=23
cfgRacTuneSshPort=22
cfgRacTuneIpRangeEnable=0
cfgRacTuneIpRangeAddr=192.168.1.1
cfgRacTuneIpRangeMask=255.255.255.0
cfgRacTuneIpBlkEnable=0
cfgRacTuneIpBlkFailCount=5
cfgRacTuneIpBlkFailWindow=60
cfgRacTuneIpBlkPenaltyTime=300
cfgRacTuneTimezoneOffset=0
cfgRacTuneDaylightOffset=0
```

cfgRacSecurity

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

Descripción

Define los valores de configuración relacionados con la función de solicitud de firma de certificado (CSR) SSL del CMC.

 **NOTA:** Para poder generar una solicitud CSR desde el CMC, en primer lugar es necesario configurar las propiedades de este grupo.

Para obtener más información sobre la generación de solicitudes de firma de certificado por medio de RACADM, consulte [sslcsrgen](#).

cfgRacSecCsrKeySize

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

Opciones de configuración: 512, 1024, 2048

Valor predeterminado: 1024

cfgRacSecCsrCommonName

Especifica el nombre común (CN) de la CSR.

Opciones de configuración: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrOrganizationName

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

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrOrganizationUnit

Especifica la unidad organizacional (OU) de la CSR.

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrLocalityName

Especifica la localidad (L) de la CSR.

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrStateName

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

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrCountryCode

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

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

cfgRacSecCsrEmailAddr

Especifica la dirección de correo electrónico de la CSR.

Valor legal: cadena de hasta 254 caracteres.

Valor predeterminado: [nulo]

Ejemplo

```
racadm config -g cfgRacSecurity
```

```
cfgRacSecCsrKeySize=1024
cfgRacSecCommonName=
cfgRacSecOrganizationName=
cfgRacSecOrganizationUnit=
cfgRacSecLocalityName=
cfgRacSecStateName=
cfgRacSecCountryCode=
cfgRacSecEmailAddr=
```

cfgActiveDirectory

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Configura las propiedades de Microsoft® Active Directory®.

cfgADEnable

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

Opciones de configuración: 1 (verdadero), 0 (falso)

Valor predeterminado: 0

cfgADRacDomain

Especifica el dominio de Active Directory en el que reside el CMC.

Opciones de configuración: cadena de hasta 254 caracteres sin espacios.

Valor predeterminado: [nulo]

cfgADRootDomain

Especifica el dominio raíz del bosque de dominio.

Opciones de configuración: cadena de hasta 254 caracteres sin espacios.

Valor predeterminado: [nulo]

cfgADRacName

Especifica el nombre del CMC tal como se ha registrado en el bosque de Active Directory.

Opciones de configuración: cadena de hasta 254 caracteres sin espacios.

Valor predeterminado: [nulo]

cfgADAuthTimeout

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

Rango de configuración: de 15 a 300

Valor predeterminado: 120

cfgADType

Indica el tipo de esquema (ampliado o estándar) a utilizar con Active Directory.

Opciones de configuración: 1 (ampliado), 2 (estándar)

Valor predeterminado: 1 (ampliado)

cfgADSpecifyServerEnable

Permite activar o desactivar y especificar un servidor LDAP o de catálogo global. Para especificar la dirección IP, utilice los comandos `cfgADDomainController` o `cfgADGlobalCatalog`.

Opciones de configuración: 1 (activado), 0 (desactivado)

Valor predeterminado: 0 (desactivado)

cfgADDomainController

Especifica el servidor LDAP desde el que el CMC deberá obtener los nombres de usuarios. **Debe utilizarse con el comando `cfgADSpecifyServerEnable`.**

Valor legal: dirección IP válida o nombre completo de dominio (FQDN).

cfgADGlobalCatalog

Especifica el servidor de catálogo global desde el que el CMC deberá obtener los nombres de usuarios. **Debe utilizarse con el comando `cfgADSpecifyServerEnable`.**

Valor legal: dirección IP válida o FQDN.

Ejemplo

```
racadm getconfig -g cfgActiveDirectory
```

```
cfgADEnable=1
cfgADRootDomain=
cfgADRootDomain=help
cfgADRootName=
cfgADRootAuthTimeout=300
cfgADRootType=0x4
cfgADRootSpecifyServerEnable=1
cfgRacADDomainController=192.168.1.1
cfgRacADGlobalCatalog=127.0.0.1
```

cfgStandardSchema

 **NOTA:** Utilice este objeto con los subcomandos **config** o **getconfig**.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Define la configuración del esquema estándar de Active Directory.

cfgSSADRoleGroupIndex

Es de sólo lectura. Muestra el índice del grupo de funciones según se registró en Active Directory.

Rango de configuración: de 1 a 5

cfgSSADRoleGroupName

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

Opciones de configuración: cadena de hasta 254 caracteres sin espacios.

Valor predeterminado: [nulo]

cfgSSADRoleGroupDomain

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

Opciones de configuración: cadena de hasta 254 caracteres sin espacios.

cfgSSADRoleGroupPrivilege

Especifica los números de máscaras de bits (consulte [tabla B-1](#)) para definir los privilegios de autoridad según funciones en un grupo de funciones.

Rango de configuración: de 0x00000000 a 0x000001ff

Valor predeterminado: [nulo]

Ejemplo

```
racadm getconfig -g cfgStandardSchema
```

```
# cfgSSADRoleGroupIndex=1
cfgSSADRoleGroupName=blsys-1
cfgSSADRoleGroupDomain=
cfgSSADRoleGroupPrivilege=3081
```

cfgChassisPower

 **NOTA:** Utilice este objeto con los subcomandos `config` o `getConfig`.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción `-o`.

Descripción

Muestra información sobre la alimentación del chasis y permite configurarla.

`cfgChassisInPower`

Es de sólo lectura. Indica los datos de consumo de alimentación de CA de entrada acumulados (en vatios y BTU/h), capturados de todas las unidades de suministro de energía operativas y en buen estado del chasis.

`cfgChassisPeakPower`

Es de sólo lectura. Indica el consumo máximo de alimentación (en vatios) a nivel de sistema desde que el valor fue borrado por última vez por un usuario.

`cfgChassisPeakPowerTimestamp`

Es de sólo lectura. Indica la fecha y hora registradas cuando se produjo el valor máximo de alimentación del sistema.

`cfgChassisMinPower`

Es de sólo lectura. Indica el valor de consumo mínimo de alimentación (en vatios) a nivel de sistema durante el tiempo transcurrido desde que el valor se borró por última vez.

`cfgChassisMinPowerTimestamp`

Es de sólo lectura. Indica la fecha y hora registradas cuando se produjo la mínima alimentación del sistema.

`cfgChassisPowerStatus`

Es de sólo lectura. Indica el estado de alimentación del chasis.

Opciones de configuración: 1 (otro), 2 (desconocido), 3 (en buen estado), 4 (no crítico), 5 (crítico), 6 (no recuperable)

`cfgChassisRedundantState`

Es de sólo lectura. Activa o desactiva la redundancia de alimentación del chasis.

Valores: 0 (ninguno), 1 (completo)

`cfgChassisPowerCap`

Indica el límite del consumo máximo de alimentación (en vatios) de todo el chasis. El comando generará un error si la regulación de la cuchilla es necesaria para alcanzar el objetivo de alimentación según el valor para esta configuración.

Rango de configuración: de 2768 a 7928 vatios

Valor predeterminado: 7928 vatios

`cfgChassisPowerCapF`

Indica el límite del consumo máximo de alimentación (en vatios) de todo el chasis. Use `cfgChassisPowerCapF` cuando se cambie el consumo de energía, sin importar que se requiera la regulación de la cuchilla o no.

Rango de configuración: de 2768 a 7928 vatios

Valor predeterminado: 7928 vatios

cfgChassisPowerCapBTU

Indica el límite del consumo máximo de alimentación (en BTU/h) de todo el chasis. El comando generará un error si la regulación de la cuchilla es necesaria para alcanzar el objetivo de alimentación según el valor para esta configuración.

Rango de configuración: 9445-27051 BTU/h

Valor predeterminado: 27051 BTU/h

cfgChassisPowerCapFBTU

Indica el límite del consumo máximo de alimentación (en BTU/h) de todo el chasis. Use cfgChassisPowerCapFBTU cuando se cambie el consumo de energía, sin importar que se requiera la regulación de la cuchilla o no.

Rango de configuración: 9445-27051 BTU/h

Valor predeterminado: 27051 BTU/h

cfgChassisPowerCapPercent

Indica el límite de consumo de energía como un porcentaje. El porcentaje se computa en forma matemática como la alimentación mínima + (porcentaje* (alimentación máxima - alimentación mínima)). El comando generará un error si la regulación de la cuchilla es necesaria para alcanzar el objetivo de alimentación según el valor para esta configuración.

Rango de configuración: 0-100

Valor predeterminado: 100

cfgChassisPowerCapFPercent

Indica el límite de consumo de energía como un porcentaje. El porcentaje se computa en forma matemática como la alimentación mínima + (porcentaje* (alimentación máxima - alimentación mínima)). Use cfgChassisPowerCapFPercent cuando se cambie el consumo de energía, sin importar que se requiera la regulación de la cuchilla o no.

Rango de configuración: 0-100

Valor predeterminado: 100

cfgChassisRedundancyPolicy

Define la política de redundancia del chasis.

Opciones de configuración: 0 (sin redundancia), 1 (redundancia de CA), 2 (redundancia de suministro de energía).

Valor predeterminado: 0 (sin redundancia)

cfgChassisDynamicPSUEngagementEnable

Activa o desactiva la conexión dinámica.

Opciones de configuración: 0 (desactivado), 1 (activado)

Valor predeterminado: 0 (desactivado)

cfgChassisInMaxPowerCapacity

Es de sólo lectura. Indica el presupuesto de alimentación total del chasis (en vatios) que está disponible para la operación del chasis

cfgChassisInRedundancyReserve

Es de sólo lectura. Indica la cantidad de alimentación redundante (en vatios) en reserva que se puede usar en caso de falla de la red de CA o de una unidad de suministro de energía. Si la política de redundancia se define con el valor 0, este valor será 0 (sin redundancia).

cfgChassisInPowerServerAllocation

Es de sólo lectura. Indica la potencia acumulada (en vatios) asignada a los servidores.

Valor predeterminado: 7928

cfgChassisInfrastructureInPowerAllocation

Es de sólo lectura. Indica la cantidad calculada acumulada de consumo de potencia de CC de salida (en vatios) que se determina a partir de una unidad reemplazable en el campo (FRU) en los módulos de hardware del chasis.

cfgChassisTotalInPowerAvailable

Es de sólo lectura. Indica la cantidad de energía disponible (en vatios) para ser utilizada por el chasis.

cfgChassisStandbyInPowerCapacity

Sólo lectura. Indica la cantidad de alimentación (en vatios) que está disponible para encender cualquier módulo de hardware que esté, ya sea, agregado al chasis o encendido (si ya está presente en el chasis).

cfgChassisPowerClear

Es de **sólo escritura**. Para restablecer `cfgChassisMinPower` y `cfgChassisMaxPowerCapacity`, defina este objeto como 1.

cfgChassisPowerClearTimestamp

Sólo lectura. Fecha y hora cuando se restablecieron `cfgChassisMinPower` y `cfgChassisMaxPowerCapacity`.

cfgChassisPowerButtonEnable

Indica si el botón de encendido del chasis está activado o desactivado.

Valores: 0 (desactivado), 1 (activado)

cfgSystemEnergyConsumptionClear

Es de **sólo escritura**. Para restablecer las estadísticas de energía, configure este valor en 1.

Ejemplos

```
racadm getconfig -g cfgChassisPower
# cfgChassisInPower=0 W | 0 BTU/hr
# cfgChassisPeakPower=0 W
# cfgChassisPeakPowerTimestamp=06:32:55 26/01/09
# cfgChassisMinPower=0 W
# cfgChassisMinPowerTimestamp=06:32:55 26/01/09
# cfgChassisPowerStatus=5
# cfgChassisRedundantState=0
cfgChassisPowerCap=7928 W
cfgChassisPowerCapF=7928 W
cfgChassisPowerCapFBTU=200 BTU/hr
cfgChassisPowerCapFBTU=200 BTU/hr
cfgChassisPowerCapPercent =10%
cfgChassisPowerCapFPercent =10%
cfgChassisRedundancyPolicy=0
cfgChassisDynamicPSUEngagementEnable=0
# cfgChassisInMaxPowerCapacity=0 W
# cfgChassisInRedundancyReserve=0 W
# cfgChassisInPowerServerAllocation=0 W
# cfgChassisInfrastructureInPowerAllocation=51 W
# cfgChassisTotalInPowerAvailable=0 W
# cfgChassisStandbyInPowerCapacity=0 W
# cfgChassisPowerClear=***** (Write-Only)
# cfgChassisPowerClearTimestamp=18:00:00 31/12/69
cfgChassisPowerButtonEnable=1
```

```
cfgSystemEnergyConsumptionClear = ****(Write-Only)
| racadm config -g cfgChassisPower -o cfgChassisPowerClear 1
```

Borra `cfgChassisMinPower` y `cfgChassisPeakPower`.

cfgServerInfo

 **NOTA:** Utilice este objeto con los subcomandos `config` o `getconfig`.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción `-o`.

Descripción

Muestra información sobre un servidor del chasis y permite configurarlo.

cfgServerIndex

Es de sólo lectura. Muestra el nombre de índice del servidor.

cfgServerSlotNumber

Es de sólo lectura. Indica la ubicación del servidor especificado (1-16) en el chasis.

cfgServerServiceTag

Es de sólo lectura. Muestra la etiqueta de servicio del servidor especificado.

cfgServerName

Indica el nombre del servidor especificado.

Opciones de configuración: cadena de caracteres alfanuméricos, puntos y guiones; 15 caracteres como máximo.

Valor predeterminado: `SLOT-<número de ranura>`

cfgServerBmcMacAddress

Es de sólo lectura. Muestra la dirección MAC de BMC del servidor especificado.

cfgServerNic1MacAddress

Es de sólo lectura. Muestra la dirección MAC de la tarjeta de interfaz de red del servidor.

cfgServerNic2MacAddress

Es de sólo lectura. Muestra la dirección MAC de la tarjeta de interfaz de red del servidor.

cfgServerPriority

Define el nivel de prioridad asignado al servidor en el chasis para fines de creación del presupuesto de alimentación.

Rango de configuración: prioridad descendente de 1 a 9, donde 1 representa la máxima prioridad

Valor predeterminado: 1

cfgServerNicEnable

Activa o desactiva el canal LAN.

Opciones de configuración: 0 (desactivar), 1 (activar)

cfgServerIPMIOverLanEnable

Activa o desactiva el canal LAN de IPMI.

Opciones de configuración: 0 (desactivar), 1 (activar)

#cfgServerPowerBudgetAllocation

Es de sólo lectura. Muestra la asignación de alimentación actual para el servidor.

cfgServerDNSRegisterIMC

Activa o desactiva el registro del nombre DNS para el controlador de administración integrado, iDRAC.

Opciones de configuración: 0 (desactivar), 1 (activar)

cfgServerDNSIMCName

Muestra el nombre dominio de DNS para el controlador de acceso remoto integrado, iDRAC.

#cfgServerRootPassword

Es de sólo escritura. Muestra la contraseña para el iDRAC como una serie de asteriscos (*). Una vez que se define la propiedad, no puede visualizarse.

Ejemplo

```
racadm getconfig -g cfgServerInfo -i 1
```

```
# cfgServerInfoIndex=1
cfgServerSlotNumber=1
# cfgServerServiceTag=JGPRQ61
cfgServerName=Server-1
# cfgServerBmcMacAddress=00:11:43:FD:B7:2A
# cfgServerNic1MacAddress=00:11:43:FD:B7:2A
# cfgServerNic2MacAddress=00:11:43:FD:B7:2A
# cfgServerNic3MacAddress=00:11:43:FD:B7:2A
# cfgServerNic4MacAddress=00:11:43:FD:B7:2A
cfgServerPriority=1
cfgServerNicEnable=1
cfgServerIPMIOverLanEnable=1
# cfgServerPowerBudgetAllocation=200W
```

```
racadm getconfig -g cfgServerInfo -i 9
```

```
# cfgServerInfoIndex=9
cfgServerSlotNumber=9
# cfgServerServiceTag=N/A
cfgServerName=Server-9
# cfgServerBmcMacAddress=N/A
# cfgServerNic1MacAddress=N/A
# cfgServerNic2MacAddress=00:11:43:FD:B7:2A
cfgServerPriority=1
cfgServerNicEnable=N/A
cfgServerIPMIOverLanEnable=N/A
# cfgServerPowerBudgetAllocation=N/A
```

cfgKVMInfo

 **NOTA:** Utilice este objeto con los subcomandos `config` o `getconfig`.

 **NOTA:** Para utilizar esta propiedad de objeto debe contar con privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Puede configurar cualquier valor que no aparezca precedido por el símbolo de almohadilla/numeral (#) en el mensaje de salida. Para modificar un objeto que puede configurarse, utilice la opción **-o**.

Descripción

Muestra información del iKVM y lo configura.

cfgKVMAccessToCMCEnable

Activa o desactiva el acceso a la consola Dell CMC en el iKVM.

Opciones de configuración: 1 (activar), 0 (desactivar)

cfgKVMFrontPanelEnable

Activa o desactiva el acceso al panel frontal en el iKVM.

Opciones de configuración: 1 (activar), 0 (desactivar)

Ejemplo

```
racadm getconfig -g cfgKVMInfo
```

```
cfgKVMAccessToCMCEnable=1  
cfgKVMFrontPanelEnable=1
```

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso de la interfaz del panel LCD

Guía del usuario

- [Navegación de la pantalla LCD](#)
- [Diagnóstico](#)
- [Solución de problemas del hardware LCD](#)
- [Mensajes de la pantalla LCD del panel frontal](#)
- [Mensajes de error de la pantalla LCD](#)
- [Información de estado del servidor y módulo de LCD](#)

El panel LCD puede utilizarse para tareas de configuración y diagnóstico y para obtener información de estado acerca del chasis y el contenido del mismo.

Navegación de la pantalla LCD

Utilice los botones situados a la derecha de la pantalla LCD para ejecutar funciones en el panel LCD. Los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha cambian los iconos u opciones de menú seleccionados en la pantalla. La opción seleccionada aparece con un fondo o borde de color azul claro.

El botón del centro activa la opción seleccionada.

Si la longitud de los mensajes que se muestran en la pantalla LCD excede la capacidad de la pantalla, utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por el texto en esas direcciones.

Los iconos que se describen en [tabla C-1](#) se utilizan para navegar entre las pantallas LCD:

Tabla C-1. Iconos de navegación del panel LCD

Icono normal	Icono resaltado	Nombre y descripción del icono
		Atrás. Seleccione y presione el botón central para regresar a la pantalla anterior.
		Aceptar/Sí. Seleccione y presione el botón central para aceptar un cambio y regresar a la pantalla anterior.
		Omitir/Siguiente. Seleccione y presione el botón central para omitir los cambios y avanzar a la siguiente pantalla.
		No. Seleccione y presione el botón central para responder "No" a una pregunta y avanzar a la siguiente pantalla.
 O bien: 		Girar. Seleccione y presione el botón central para alternar entre las vistas gráficas de la parte frontal y posterior del chasis. NOTA: El fondo de color ámbar indica que la vista opuesta contiene errores.
		Identificación de componente. El LED de color azul parpadea en un componente. NOTA: Habrá un rectángulo azul parpadeando cerca de este icono cuando se activa la Identificación del componente .

Menú principal

Desde el menú **Principal** puede acceder a una de las siguientes pantallas:

- 1 **Menú de configuración de LCD:** seleccione el idioma que se utilizará y la pantalla LCD que aparecerá cuando no se utilice el LCD.
- 1 **Servidor:** muestra información sobre el estado de los servidores.
- 1 **Gabinete:** muestra información sobre el estado del chasis.

1. Utilice los botones de flecha hacia arriba y abajo para resaltar una opción.
2. Para activar la opción seleccionada, presione el botón central.

Menú de configuración del LCD

El menú **Configuración de LCD** muestra diversas opciones que pueden configurarse:

- 1 **Configuración de idioma:** seleccione el idioma que desea utilizar para el texto de la pantalla LCD y los mensajes.
- 1 **Pantalla predeterminada:** elija la pantalla que aparece cuando el panel LCD está inactivo.

1. Utilice los botones de flecha hacia arriba y abajo para resaltar una opción del menú o seleccione el icono **Atrás** si desea regresar al menú **Principal**.
2. Para activar la opción seleccionada, presione el botón central.

Pantalla de configuración de idioma

La pantalla **Configuración de idioma** permite seleccionar el idioma de los mensajes del panel LCD. El idioma activo aparece resaltado con un fondo de color azul claro.

1. Utilice los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha para resaltar el idioma deseado.
2. Presione el botón central. Aparecerá el icono **Aceptar resaltado**.
3. Para confirmar los cambios, presione el botón del centro. Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

La opción **Pantalla predeterminada** permite cambiar la pantalla que aparece en el panel LCD cuando se encuentra inactivo. La pantalla predeterminada de fábrica es el **Menú principal**. Puede seleccionar una de las siguientes pantallas:

- 1 **Menú principal**
- 1 **Estado del servidor** (vista frontal del chasis)
- 1 **Estado del módulo** (vista posterior del chasis)
- 1 **Personalizado** (logotipo de Dell con el nombre del chasis)

La pantalla actualmente activa aparece resaltada en azul.

1. Utilice los botones de flecha hacia arriba y abajo para resaltar la pantalla que desea definir como predeterminada.
2. Presione el botón central. El icono **Aceptar** quedará resaltado.
3. Presione el botón central nuevamente para confirmar los cambios. Aparecerá la **Pantalla predeterminada**.

Pantalla de estado gráfico del servidor

La pantalla **Estado gráfico del servidor** muestra iconos para cada servidor instalado en el chasis e indica su estado general. La condición del servidor se indica mediante el color del icono:

- 1 **Gris:** el servidor está apagado y no presenta errores
- 1 **Verde:** el servidor está encendido y no presenta errores
- 1 **Ámbar:** el servidor presenta uno o más errores
- 1 **Negro:** no se registra la presencia del servidor

El rectángulo azul que parpadea alrededor del icono del servidor indica el servidor seleccionado.

Para acceder a la pantalla **Estado gráfico del módulo**:

1. Seleccione el icono de giro.
2. Presione el botón central.

Para ver la pantalla de estado de un servidor:

1. Utilice los botones de flecha para resaltar el servidor deseado.
2. Presione el botón central. Aparecerá la pantalla **Estado del servidor**.

Para regresar al Menú principal:

1. Utilice los botones de flecha para resaltar el icono **Atrás**.
2. Presione el botón central.

Pantalla de estado gráfico del módulo

La pantalla **Estado gráfico del módulo** muestra todos los módulos instalados en la parte posterior del chasis y ofrece un resumen sobre la condición de cada módulo. La condición del módulo se indica mediante el color de cada icono, tal como se muestra a continuación:

- 1 Gris: el módulo está apagado o en espera y no presenta errores
- 1 Verde: el módulo está encendido y no presenta errores
- 1 Ámbar: el módulo presenta uno o más errores
- 1 Negro: no se registra la presencia del módulo

El rectángulo azul que parpadea alrededor del icono del módulo indica el módulo seleccionado.

Para acceder a la pantalla **Estado gráfico del servidor**:

1. Seleccione el icono de giro.
2. Presione el botón central.

Para ver la pantalla de estado de un módulo:

1. Utilice los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia derecha para resaltar el módulo deseado.
2. Presione el botón central. Aparecerá la pantalla **Estado del módulo**.

Para regresar al **Menú principal**:

1. Utilice los botones de flecha para resaltar el icono **Atrás**.
2. Presione el botón central. Aparecerá el **Menú principal**.

Pantalla del menú Gabinete

Esta pantalla le permite acceder a las siguientes pantallas:

- 1 Pantalla **Estado del módulo**
- 1 Pantalla **Estado del gabinete**
- 1 Pantalla **Resumen de IP**
- 1 **Menú principal**

1. Utilice los botones de navegación para resaltar la opción deseada (seleccione el icono **Atrás** para regresar al **Menú principal**).
2. Presione el botón central. Aparecerá la pantalla seleccionada.

Pantalla de estado del módulo

La pantalla **Estado del módulo** muestra la información y los mensajes de error de un módulo. Consulte "[Información de estado del servidor y módulo de LCD](#)".

y "[Mensajes de error de la pantalla LCD](#)" para ver los mensajes que pueden aparecer en esta pantalla.

Utilice las teclas de flecha hacia arriba y abajo para desplazarse por los mensajes. Utilice las teclas de flecha hacia la izquierda y la derecha para desplazarse por un mensaje que no cabe la pantalla.

Seleccione el icono **Atrás** y presione el botón central para regresar a la pantalla **Estado gráfico del módulo**.

Pantalla Estado del gabinete

La pantalla Estado del gabinete muestra información y mensajes de error del gabinete. Consulte "[Mensajes de error de la pantalla LCD](#)" para ver los mensajes que pueden aparecer en esta pantalla.

Utilice las teclas de flecha hacia arriba y abajo para desplazarse por los mensajes. Utilice las teclas de flecha hacia la izquierda y la derecha para desplazarse por un mensaje que no cabe la pantalla.

Seleccione el icono **Atrás** y presione el botón central para regresar a la pantalla **Estado del gabinete**.

Pantalla de resumen de IP

La pantalla **Resumen de IP** muestra información de IP del CMC y el iDRAC de cada servidor instalado.

Utilice los botones de flecha hacia arriba y abajo para desplazarse por la lista. Utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por un mensaje seleccionado cuya longitud excede la pantalla.

Utilice los botones de flecha hacia arriba y abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Diagnóstico

El panel LCD le permite diagnosticar problemas de cualquier servidor o módulo del chasis. Si existe un problema o una falla en el chasis o en cualquier servidor u otro módulo del chasis, el indicador de estado del panel LCD parpadeará con una luz de color ámbar. En el **Menú principal**, un icono parpadearante con fondo de color ámbar aparece junto la opción correspondiente -Servidor o Gabinete- que permite acceder al servidor o módulo fallido.

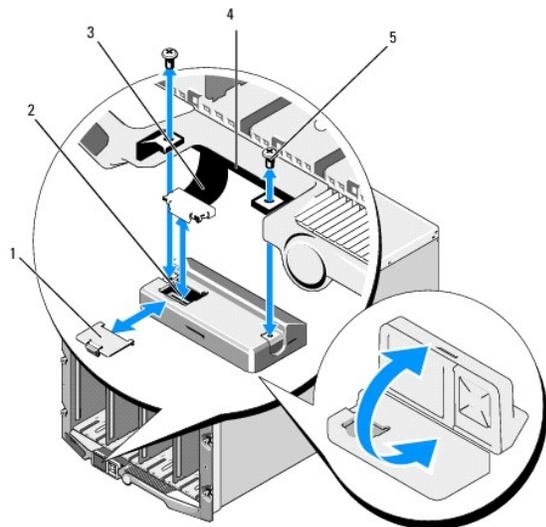
Seguindo los iconos que parpadean en color ámbar a través del sistema de menús de la pantalla LCD, es posible visualizar la pantalla de estado y los mensajes de error de la opción que presenta el problema.

Los mensajes de error del panel LCD pueden eliminarse si se elimina el módulo o servidor que causa el problema o si se borra el registro de hardware correspondiente al módulo o al servidor. Para los errores de servidor, utilice la interfaz web de iDRAC o la interfaz de línea de comandos a fin de borrar el Registro de sucesos del sistema (SEL) del servidor. Para los errores de chasis, utilice la interfaz web del CMC o la interfaz de línea de comandos a fin de borrar el registro de hardware.

Solución de problemas del hardware LCD

Si está teniendo problemas con el LCD que estén relacionados con la utilización del CMC, use las siguientes opciones de solución de problemas de hardware para determinar si existe un problema con el hardware LCD o con la conexión.

Figura C-1. Extracción e instalación del módulo LCD



1 | Cubierta de cables

2 | Módulo LCD

3	Cable plano	4	Bisagras (2)
5	Tornillos (2)		

Síntoma	Problema	Acción de recuperación
Mensaje de alerta de pantalla CMC Not Responding (CMC no responde y el LED) está parpadeando en color ámbar	Pérdida de la comunicación desde el CMC al panel anterior del LCD	Verifique que el CMC se esté iniciando; luego, reinicie el CMC a través de GUI o los comandos de RACADM.
Mensaje de alerta de pantalla CMC Not Responding (CMC no responde y el LED) y el LED de color ámbar oscuro está apagado	El panel anterior del LCD permanece con bloqueo de inicio durante la transferencia por falla del CMC	Desconecte y vuelva a conectar la placa de circuito del panel anterior al cable del panel de E/S desde el panel anterior. Restablezca el CMC a través de GUI o de los comandos de RACADM.
El LED parpadea en color ámbar o está en blanco.	El LCD no está conectado correctamente al cable de la placa de circuito del panel anterior o es fallido; o el panel anterior es fallido.	Revise el registro de hardware a través de GUI o de los comandos de RACADM. Busque un mensaje que diga: Control Panel TFT Cable: Cable sensor for Control Panel, configuration error was asserted (Cable TFT de panel de control: sensor de cable para panel de control, el error de configuración se confirmó) Reemplace el panel anterior.
El texto de la pantalla está codificado	Pantalla LCD defectuosa	Reemplace el panel anterior.
Mensaje de pantalla LCD No CMC Found (No se encontró CMC)	No hay ningún CMC en el chasis	Inserte un CMC en el chasis o reemplace el CMC existente si no funciona.
LCD en blanco y LED apagado	El cable de la placa de circuito del panel anterior o el cable del panel de E/S no están conectados correctamente; o uno o ambos son fallidos.	Revise el registro de hardware a través de GUI o de los comandos de RACADM. Busque mensajes que digan: Control Panel FPC Cable: Cable sensor for Control Panel, configuration error was asserted (Cable FPC de panel de control: sensor de cable para panel de control, el error de configuración se confirmó) Control Panel I/O Cable: Cable sensor for Control Panel, configuration error was asserted (Cable de E/S de panel de control: sensor de cable para panel de control, el error de configuración se confirmó) Asegúrese de que los cables estén correctamente conectados.

Mensajes de la pantalla LCD del panel frontal

Esta sección incluye dos apartados que muestran los mensajes de error y la información de estado que aparecen en la pantalla LCD del panel frontal.

Los *mensajes de error* de la pantalla LCD tienen un formato similar al del registro de sucesos del sistema (SEL) que se visualiza en la interfaz web o en CLI. A continuación se ilustra el formato:

```
<Gravedad> <Nombre del sensor>: <Tipo de sensor> sensor de <Entidad>, <Descripción del suceso>
```

Las tablas de la sección de errores muestran los mensajes de error y advertencia que aparecen en las diversas pantallas LCD y la causa posible del mensaje. El texto que aparece entre corchetes angulares (< >) indica que el texto puede variar.

La *información de estado* de la pantalla LCD incluye datos descriptivos sobre los módulos del chasis. Las tablas de esta sección describen la información que se muestra para cada componente.

Mensajes de error de la pantalla LCD

Tabla C-2. Pantallas de estado del CMC

Gravedad	Mensaje	Causa
Crítico	Batería del CMC <número>: Sensor de batería del CMC, se confirmó la falla	La batería de CMOS del CMC no está presente o no tiene voltaje.
Crítico	Temp de CPU del CMC <número>: Sensor de temperatura del CMC, suceso de falla	La temperatura de la CPU del CMC superó el umbral crítico.
Crítico	Temp ambiente del CMC <número>: Sensor de temperatura del CMC, suceso de falla	La temperatura ambiente del CMC superó el umbral crítico.
Advertencia	Incompatibilidad de chasis FW: el sensor de cambio de versión para la incompatibilidad de chasis, firmware o software (sistema BIOS en la ranura XX con el CMC) se confirmó.	Posible pérdida de funciones o componentes debido a la incompatibilidad de las versiones de software.
Advertencia	Incompatibilidad de chasis FW: el sensor de cambio de versión para la incompatibilidad de chasis, firmware o software (iDRAC en la ranura XX con el CMC) se confirmó.	Posible pérdida de funciones o componentes debido a la incompatibilidad de las versiones de software.

Tabla C-3. Pantalla de estado del gabinete/chasis

Gravedad	Mensaje	Causa
Crítico	Presencia de ventilador <número> de chasis: Sensor del ventilador del chasis, se confirmó la eliminación del dispositivo	Este ventilador se requiere para la correcta ventilación del gabinete o el chasis.
Advertencia	Redundancia de suministro de energía: Sensor de redundancia de suministro de energía, se confirmó la redundancia degradada	Una o más unidades de suministro de energía fallaron o fueron eliminadas y el sistema ya no admite redundancia de unidad de suministro de energía completa.
Crítico	Redundancia de suministro de energía: Sensor de redundancia de suministro de energía, se confirmó la pérdida de redundancia	Una o más unidades de suministro de energía fallaron o fueron eliminadas y el sistema ya no es redundante.
Crítico	Redundancia de suministro de energía: Sensor de redundancia de suministro de energía, no redundante: recursos insuficientes	Una o más unidades de suministro de energía fallaron o fueron eliminadas y el sistema carece de suficiente energía para mantener el funcionamiento normal. Esto puede hacer que los servidores se apaguen.
Crítico	Temp de panel de control: Sensor de temperatura del panel de control, suceso de falla	La temperatura del chasis/gabinete superó el umbral crítico.
Crítico	CMC <número> independiente: Sensor de microcontrolador del CMC, se confirmó la falta de redundancia	El CMC ya no es redundante. NOTA: Este mensaje sólo aparecerá si el CMC en espera fue retirado o falló.
Crítico	Registro de sucesos del chasis CEL: Sensor de registro de sucesos para el registro de sucesos del chasis, se confirmó la desactivación total del registro de sucesos	El CMC no puede registrar sucesos.
Crítico	Registro de sucesos del chasis CEL: Sensor de registro de sucesos para el registro de sucesos del chasis, se confirmó que el registro está lleno	El dispositivo del chasis detecta que sólo puede agregarse una entrada más al CEL antes que se llene.
Advertencia	Registro de sucesos del chasis CEL: Sensor de registro de sucesos para el registro de sucesos del chasis, se confirmó que el registro está casi lleno	El registro de sucesos del chasis se encuentra al 75% de su capacidad.

Tabla C-4. Pantallas de estado del ventilador

Gravedad	Mensaje	Causa
Crítico	Estado del ventilador <número> del chasis: Sensor del ventilador del chasis, suceso de falla	La velocidad del ventilador indicado no es suficiente para proporcionar ventilación adecuada al sistema.

Tabla C-5. Pantallas de estado del módulo de E/S

Gravedad	Mensaje	Causa
Advertencia	Estado del módulo de E/S <número>: Sensor de módulo para el módulo de E/S, se confirmó la transición de estado correcto a estado no crítico	El módulo de E/S estaba en buen estado pero actualmente presenta problemas de incompatibilidad de estructura de red o de ajuste de vínculo.
Crítico	Estado del módulo de E/S <número>: Sensor del módulo de E/S, se confirmó la transición de estado de menor gravedad a estado crítico	El módulo de E/S presenta una falla. El mismo error puede presentarse si el módulo de E/S presenta problemas térmicos.

Tabla C-6. Pantalla de estado de iKVM

Gravedad	Mensaje	Causa
Advertencia	Condición del KVM local: Sensor de módulo para el KVM local, se confirmó la transición del estado no crítico a correcto	Falla menor, por ejemplo, firmware dañado.
Crítico	Condición del KVM local: Sensor de módulo para el KVM local, se confirmó la transición del estado de menor gravedad a crítico	Falla de enumeración del host USB o falla de OSCAR.

No recuperable	Condición del KVM local: Sensor de módulo para el KVM local, se confirmó la transición al estado no recuperable	Falla de RIP serie o de chip del host USB.
----------------	---	--

Tabla C-7. Pantallas de estado de la unidad de suministro de energía

Gravedad	Mensaje	Causa
Crítico	Unidad de suministro de energía <número>: Sensor del suministro de energía, se confirmó la falla	Se produjo una falla en la unidad de suministro de energía.
Crítico	Unidad de suministro de energía <número>: Sensor del suministro de energía, se confirmó la pérdida de energía	Pérdida de energía de CA o cable de CA sin conectar.

Tabla C-8. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Advertencia	Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de advertencia	La temperatura ambiente del servidor superó un umbral de advertencia.
Crítico	Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de falla	La temperatura ambiente del servidor superó un umbral de falla.
Crítico	Batería CMOS de la placa del sistema: sensor de la batería de la placa del sistema, se confirmó una falla	La batería de CMOS no está presente o no tiene voltaje.
Advertencia	Nivel de sistema de la placa del sistema: sensor de corriente de la placa del sistema, suceso de advertencia	La corriente superó un umbral de advertencia.
Crítico	Nivel de sistema de la placa del sistema: sensor de corriente de la placa del sistema, suceso de falla	La corriente superó un umbral de falla.
Crítico	CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la unidad de suministro de energía <número>, se confirmó el estado declarado	El voltaje está fuera del rango permitido.
Crítico	<Nombre del sensor de voltaje> de la placa del sistema: sensor de voltaje de la placa del sistema, se confirmó el estado declarado	El voltaje está fuera del rango permitido.
Crítico	CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la unidad de suministro de energía <número>, se confirmó el estado declarado	El voltaje está fuera del rango permitido.
Crítico	Estado de la CPU <número>: Sensor de procesador para la CPU <número>, se confirmó IERR	Falla de la CPU.
Crítico	Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó un disparo térmico	La CPU se sobrecalentó.
Crítico	Estado de la CPU <número>: Sensor de procesador para la CPU <número>, se confirmó un error de configuración	Tipo de procesador o ubicación incorrectos.
Crítico	Estado de la CPU <número>: Sensor de procesador para la CPU <número>, no se confirmó la presencia	La CPU requerida no se encuentra o no está presente.
Crítico	Tarjeta vertical de vídeo de la placa del sistema: sensor de módulo de la placa del sistema, se confirmó el retiro del dispositivo	El módulo requerido fue retirado.
Crítico	Estado de la tarjeta intermediaria B <número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria B <número de ranura>, se confirmó un error de instalación	Se instaló una tarjeta intermedia incorrecta para la estructura de red de E/S.
Crítico	Estado de la tarjeta intermediaria C <número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria C <número de ranura>, se confirmó un error de instalación	Se instaló una tarjeta intermedia incorrecta para la estructura de red de E/S.
Crítico	Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se retiró la unidad	La unidad de almacenamiento fue eliminada.
Crítico	Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se confirmó una falla de la unidad	Se produjo una falla en la unidad de almacenamiento.
Crítico	Protección contra fallas PFault de la placa del sistema: sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Este suceso se genera cuando los voltajes de la placa del sistema no se encuentran en los niveles normales.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó que el temporizador ha expirado	El temporizador de vigilancia de iDRAC expira sin que defina una acción.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó un reinicio	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de reiniciar.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó el apagado	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de apagado.
Crítico	Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó un ciclo de encendido	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de ciclo de encendido.
Crítico	Registro de sucesos de la placa del sistema: sensor de registro de sucesos de la placa del sistema, se confirmó que el registro está lleno	El dispositivo de registro de sucesos del sistema detecta que sólo se podrá agregar una anotación al registro antes de que se llene.
Advertencia	Error corregible ECC: Sensor de memoria, se confirmó el ECC corregible (<Ubicación del módulo DIMM>)	Los errores de ECC que pueden corregirse alcanzaron un índice crítico.
Crítico	Error no corregible ECC: Sensor de memoria, se confirmó el ECC no corregible (<Ubicación del módulo DIMM>)	Se detectó un error ECC incorregible.

Crítico	Rev. de canal de E/S: sensor de sucesos críticos, se confirmó una NMI?de revisión de canal de E/S	Se genera una interrupción crítica en el canal de E/S.
Crítico	Error de paridad de PCI: sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de paridad en el bus PCI.
Crítico	Error de sistema de PCI: Sensor de sucesos críticos, se confirmó SERR de PCI (<Número de ranura o ID de dispositivo PCI>)	El dispositivo detectó un error de PCI.
Crítico	Registro SBE desactivado: sensor de registro de sucesos, se confirmó la desactivación del registro de errores corregibles de memoria	El registro de errores de único bit se desactiva cuando se registran demasiados SBE.
Crítico	Desactivación de registro: sensor del registro de sucesos, se confirmó la desactivación de todo registro de sucesos	Todo registro de errores está desactivado.
No recuperable	Error de protocolo de CPU: sensor de procesador, se confirmó la transición a estado no recuperable	El protocolo del procesador ingresó a un estado no recuperable.
No recuperable	PERR de bus de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	El PERR de bus del procesador ingresó a un estado no recuperable.
No recuperable	Error de inicialización de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	La inicialización del procesador ingresó a un estado no recuperable.
No recuperable	Revisión de máquina de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable	La revisión de máquina del procesador ingresó a un estado no recuperable.
Crítico	Memoria de reserva: Sensor de memoria, se confirmó la pérdida de redundancia (<Ubicación del módulo DIMM>)	El repuesto de la memoria ya no es redundante.
Crítico	Memoria duplicada: Sensor de memoria, se confirmó la pérdida de redundancia (<Ubicación del módulo DIMM>)	La memoria duplicada ya no es redundante.
Crítico	RAID de memoria: Sensor de memoria, se confirmó la pérdida de redundancia (<Ubicación del módulo DIMM>)	La memoria RAID ya no es redundante.
Advertencia	Se agregó memoria: sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria agregado.
Advertencia	Se retiró memoria: no se confirmó la presencia del sensor de memoria (<ubicación del DIMM>)	Se quitó el módulo de memoria.
Crítico	Error de configuración de la memoria: Sensor de memoria, se confirmó un error de configuración (<Ubicación del módulo DIMM>)	La configuración de la memoria no es correcta para el sistema.
Advertencia	Ganancia de redundancia de memoria: Sensor de memoria, se confirmó la redundancia degradada (<Ubicación del módulo DIMM>)	La redundancia de la memoria es de bajo nivel aunque no se perdió.
Crítico	Error fatal de PCIE: sensor de sucesos críticos, se confirmó un error fatal de bus	Se detectó un error fatal en el bus de PCIE.
Crítico	Error de chipset: sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de chip.
Advertencia	Advertencia de ECC de mem: Sensor de memoria, se confirmó la transición de estado correcto a estado no crítico (<Ubicación del módulo DIMM>)	Los errores corregibles ECC han aumentado por encima de la frecuencia normal.
Crítico	Advertencia de ECC de mem: Sensor de memoria, se confirmó la transición de estado crítico a estado de menor gravedad (<Ubicación del módulo DIMM>)	Los errores de ECC que pueden corregirse alcanzaron un índice.
Crítico	Error de POST de la placa base: Sensor de POST de la placa base, se confirmó un error fatal de POST <información adicional del error>	Consulte el manual de servicio del hardware para obtener más información sobre los errores de la POST del BIOS.
Crítico	Error de la POST: sensor de la POST, no hay memoria instalada	No se detectó memoria en la placa
Crítico	Error de la POST: sensor de la POST, error de configuración de memoria	Se ha detectado la memoria, pero no se puede configurar
Crítico	Error de la POST: sensor de la POST, error de memoria inutilizable	Se ha configurado la memoria, pero no se puede utilizar
Crítico	Error de la POST: sensor de la POST, falló el copiado del BIOS en la RAM	Falla de copiado de BIOS en la RAM?del sistema
Crítico	Error de la POST: sensor de la POST, falló el CMOS	Error de CMOS
Crítico	Error de la POST: sensor de la POST, falló el controlador de DMA	Error del controlador de DMA
Crítico	Error de la POST: sensor de la POST, falló el controlador de interrupción	Error del controlador de interrupción
Crítico	Error de la POST: sensor de la POST, falló la actualización del temporizador	Error de actualización del temporizador
Crítico	Error de la POST: sensor de la POST, error de temporizador de intervalos programable	Error del temporizador de intervalos programable
Crítico	Error de la POST: sensor de la POST, error de paridad	Error de paridad
Crítico	Error de la POST: sensor de la POST, falló el SIO	Error de SIO
Crítico	Error de la POST: sensor de la POST, falló el controlador de teclado	Falla del controlador del teclado
Crítico	Error de la POST: sensor de la POST, falló la inicialización de interrupción de administración del sistema	Error de inicialización en la interrupción de administración del sistema
Crítico	Error de la POST: sensor de la POST, falló la prueba de apagado del BIOS	Error de la prueba de apagado del BIOS
Crítico	Error de la POST: sensor de la POST, falló la prueba de memoria del BIOS durante la POST	Error de la prueba de la memoria del BIOS durante la POST
Crítico	Error de la POST: sensor de la POST, falló la configuración de Dell Remote Access Controller	Error de configuración de Dell Remote Access Controller
Crítico	Error de la POST: sensor de la POST, falló la configuración de la CPU	Error de configuración de la CPU
Crítico	Error de la POST: sensor de la POST, configuración incorrecta de la memoria	Configuración incorrecta de la memoria
Crítico	Error de la POST: sensor de la POST, falló la POST	Error general tras el vídeo

Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware	Se detectó hardware incompatible
Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware (firmware del BMC)	El hardware es incompatible con el firmware
Crítico	Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware (incoherencia entre la CPU y el firmware del BMC)	La CPU y el firmware no son compatibles
Crítico	Sobrecalentamiento de memoria: sensor de memoria, se confirmó un ECC corregible <ubicación del DIMM>	Sobrecalentamiento del módulo de memoria
Crítico	CRC fatal de SB de memoria: sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Sur
Crítico	CRC fatal de NB de memoria: sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Norte
Crítico	Temporizador de vigilancia: sensor de vigilancia, se confirmó el reinicio	El temporizador de vigilancia hizo que el sistema se reiniciara
Crítico	Temporizador de vigilancia: sensor de vigilancia, se confirmó la expiración del temporizador	El temporizador de vigilancia expiró pero no se realizó ninguna acción
Advertencia	Ajuste de vínculo: sensor de cambios de versión, no se confirmó un cambio satisfactorio de software ni firmware	No se pudo actualizar el valor de ajuste de vínculo para lograr un funcionamiento adecuado del NIC
Advertencia	Ajuste de vínculo: sensor de cambios de versión, no se confirmó el cambio satisfactorio de hardware <número de ranura del dispositivo>	No se pudo actualizar el valor de ajuste de vínculo para lograr un funcionamiento adecuado del NIC
Crítico	Direcc. flexible/LinkT: sensor de ajuste de vínculo, se confirmó el error de programación de la dirección MAC?virtual (n.º de bus, n.º de dispositivo, n.º de función)	No se pudo programar FlexAddress para este dispositivo
Crítico	Direcc. flexible/LinkT: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción para apoyar el ajuste de vínculo o la dirección flexible (tarjeta intermediaria <ubicación>)	La ROM?de opción no admite FlexAddress ni el ajuste de vínculo.
Crítico	Direcc. flexible/LinkT: sensor de ajuste de vínculo, se confirmó un error para obtener datos de ajuste de vínculo o de dirección flexible del BMC/iDRAC	No se pudo obtener información de ajuste de vínculo ni de FlexAddress del BMC/iDRAC
Crítico	FlexAddr/LinkT: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción de dispositivo para admitir el ajuste de vínculo o dirección flexible (tarjeta intermediaria XX)	La ROM de opción de dispositivo de PCI para un NIC no admite el ajuste de vínculo o la función FlexAddress.
Crítico	FlexAddr/LinkT: sensor de ajuste de vínculo, se confirmó un error en la programación de la dirección MAC virtual (<ubicación>)	Error de BIOS para programar una dirección MAC virtual en el dispositivo del NIC proporcionado.
Crítico	Error fatal E/S: sensor de grupo ES fatal, error ES fatal (<ubicación>)	Se genera en relación con un IERR de CPU e indica qué dispositivo causó el IERR de CPU.
Advertencia	Error no fatal PCIe: sensor de grupo E/S no fatal, error PCIe (<ubicación>)	Se genera en relación con un IERR de CPU

Información de estado del servidor y módulo de LCD

Las tablas que figuran en esta sección describen las opciones de estado que se muestran en la pantalla LCD del panel frontal para cada tipo de componente del chasis.

Tabla C-9. Estado del CMC

N.º	Descripción
Nombre/Ubicación	Ejemplo: CMC1, CMC2
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Dirección IP	Sólo aparece en el CMC activo.
Versión del firmware	Sólo aparece en el CMC activo.

Tabla C-10. Estado del chasis/gabinete

N.º	Descripción
Nombre definido por el usuario	Ejemplo: "Sistema de estante Dell". Esta opción puede configurarse a través de la CLI o la interfaz gráfica del usuario del CMC
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Número de modelo	Ejemplo: "PowerEdgeM1000"
Consumo de alimentación	Consumo de energía actual en vatios
Excedente por rendimiento máximo	El valor del excedente por rendimiento máximo es la diferencia entre la Capacidad de alimentación de entrada del sistema y la Alimentación requerida para el rendimiento máximo (suma de la Alimentación de entrada máxima asignada a los servidores y la Alimentación de entrada máxima asignada a la infraestructura del chasis). El valor del Excedente por rendimiento máximo se muestra en vatios y en BTU/h.
Máxima energía	Máximo consumo de energía en vatios

Mínima energía	Mínimo consumo de energía en vatios
Temperatura ambiente	Temperatura ambiente actual en grados Celsius
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica
Modo de redundancia del CMC	No redundante o redundante
Modo de redundancia de la unidad de suministro de energía	No redundante, redundancia de CA o de CC

Tabla C-11. Estado del ventilador

N.º	Descripción
Nombre/Ubicación	Ejemplo: Ventilador1, Ventilador2, etc.
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
RPM	Velocidad actual del ventilador en RPM

Tabla C-12. Estado de la unidad de suministro de energía

N.º	Descripción
Nombre/Ubicación	Ejemplo: PSU1, PSU2, etc.
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Estado	Desconectado, conectado o en espera
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede brindar al sistema

Tabla C-13. Estado del módulo de E/S

N.º	Descripción
Nombre/Ubicación	Ejemplo: IOM A1, IOM B1.
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Estado	Encendido o apagado
Model	Modelo del módulo de E/S
Tipo de estructura de red	Tipo de sistema de red
Dirección IP	Sólo aparece si el módulo de E/S está encendido. El valor será cero para los módulos de E/S de paso.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla C-14. Estado de iKVM

N.º	Descripción
Nombre	iKVM
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Estado	Encendido o apagado
Modelo/fabricante	Descripción del modelo de iKVM.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Número de parte	Número de pieza del fabricante.
Versión del firmware	Versión del firmware del iKVM

Tabla C-15. Estado del servidor

N.º	Descripción
Nombre/Ubicación	Ejemplo: Servidor 1, Servidor 2.
Mensajes de error	Si no existen errores se muestra el mensaje "Sin errores". De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y luego las advertencias.
Nombre de la ranura	Nombre de la ranura del CMC. Ejemplo: SLOT-01. Nota: Esta opción puede configurarse a través de la CLI o la interfaz gráfica del usuario del CMC.

Nombre	Nombre de usuario configurable del servidor. Esta opción puede configurarse a través del BIOS del servidor, la CLI o la interfaz gráfica del usuario de iDRAC. Muestra si el iDRAC completó el inicio, o mostrará mensajes de inicio del iDRAC.
Número de modelo	Muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Muestra si el iDRAC completó el inicio.
Dirección IP del iDRAC	Muestra si el iDRAC completó el inicio. Si el iDRAC está configurado para DHCP y no obtuvo una IP, mostrará Adquiriendo .
Código de última publicación	Muestra el último código publicado que fue entregado por el BIOS del servidor.
Versión del BIOS	Muestra si el iDRAC completó el inicio.
Versión del firmware del iDRAC	Muestra si el iDRAC completó el inicio.
FlexAddress activado en estructuras de red: <Estructura de red>	Muestra si la función está instalada. Muestra las estructuras de red que tienen activado FlexAddress para este servidor (por ejemplo, A, B, C).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Configuración del CMC para el uso de consolas de línea de comandos

Guía del usuario

- [Consola de línea de comandos Funciones en el CMC](#)
- [Uso de una consola telnet o serie](#)
- [Uso de una consola Telnet con el CMC](#)
- [Uso de SSH con el CMC](#)
- [Configuración del software de emulación de terminal](#)
- [Conexión a módulos por medio del comando connect](#)

Esta sección proporciona información acerca de las funciones de la consola de línea de comandos (o la *consola de conexión serie/Telnet/Secure Shell*) del CMC y explica cómo configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola. Para obtener información sobre el uso de los comandos de RACADM en el CMC a través de la consola de línea de comandos, consulte [Uso de la interfaz de línea de comandos de RACADM](#).

Consola de línea de comandos Funciones en el CMC

El CMC admite las siguientes funciones de consola serie y Telnet:

- 1 Una conexión de cliente serie y hasta cuatro conexiones simultáneas de cliente Telnet
- 1 Hasta cuatro conexiones cliente Secure Shell (SSH) simultáneas
- 1 Compatibilidad para comandos de RACADM
- 1 Comando **connect** integrado para la depuración de errores de servidores y módulos de E/S
- 1 Historial y edición de línea de comandos
- 1 Control del tiempo de espera de las sesiones en todas las interfaces de consola

Uso de una consola telnet o serie

La consola Telnet o serie del CMC le permite encender, apagar o restablecer el servidor o los registros del servidor de acceso. Al conectarse a la línea de comandos del CMC, puede ingresar estos comandos:

Tabla 3-1. Comandos para la línea de comandos del CMC

Comando	Descripción
racadm	Los comandos RACADM comienzan con la palabra clave racadm seguida de un subcomando, por ejemplo, getconfig , serveraction o getsensorinfo . Consulte Uso de la interfaz de línea de comandos de RACADM para obtener información sobre el uso de RACADM.
connect	Establece conexión con un servidor o un módulo de E/S para la depuración de errores. Consulte Conexión a módulos por medio del comando connect para obtener ayuda acerca de cómo utilizar el comando connect .
exit, logout y quit	Estos comandos ejecutan la misma acción: finalizan la sesión actual y regresan a la pantalla de inicio de sesión.

Uso de una consola Telnet con el CMC

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 Telnet del sistema administrado requiere del software de emulación de terminal de la estación de administración. Para obtener más información, consulte [Configuración del software de emulación de terminal](#).

Uso de SSH con el CMC

SSH es una sesión de línea de comandos que incluye las mismas funciones de una sesión Telnet, pero con negociación de sesiones y cifrado para mejorar la seguridad. El CMC admite la versión 2 de SSH con autenticación de contraseña. SSH está activado en el CMC de manera predeterminada.

 **NOTA:** El CMC no admite la versión 1 de SSH.

Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente SSH envía un mensaje de error. El texto del mensaje depende del cliente y no es controlado por el CMC. Revise los mensajes de RACLog para determinar la causa de la falla.

 **NOTA:** `OpenSSH` se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. Si se ejecuta `OpenSSH` al invocar comandos de Windows no se obtendrá funcionalidad completa (es decir, algunas teclas no responderán y no se mostrarán gráficos). Para Linux, ejecute los servicios cliente de SSH para conectarse al CMC con cualquier intérprete.

Se admiten cuatro sesiones de SSH simultáneas. El tiempo de espera de la sesión es controlado por la propiedad `cfgSsnMgtSshIdleTimeout` (consulte [Subcomandos de RACADM](#)) o desde la página **Administración de servicios** de la interfaz web (consulte [Configuración de servicios](#)).

Activación de SSH en el CMC

SSH está activado de manera predeterminada. De no ser así, puede activarlo por medio de cualquier otra interfaz admitida.

Para obtener instrucciones sobre la activación de conexiones SSH en el CMC por medio de RACADM, consulte [config](#) y [cfgSerial](#). Para obtener instrucciones sobre la activación de conexiones SSH en el CMC por medio de la interfaz web, consulte [Configuración de servicios](#).

Cambio del puerto de SSH

Para cambiar el puerto SSH, utilice el siguiente comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <número de puerto>
```

Para obtener más información sobre las propiedades `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#).

La implementación de SSH del CMC admite varios esquemas de criptografía, según se muestra en [tabla 3-2](#).

Tabla 3-2. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS de 512-1024 bits (aleatorio) según especificación NIST
Criptografía simétrica	<ul style="list-style-type: none">1 AES256-CBC1 RIJNDAEL256-CBC1 AES192-CBC1 RIJNDAEL192-CBC1 AES128-CBC1 RIJNDAEL128-CBC1 BLOWFISH-128-CBC1 3DES-192-CBC1 ARCFOUR-128
Integridad de mensaje	<ul style="list-style-type: none">1 HMAC-SHA1-1601 HMAC-SHA1-961 HMAC-MD5-1281 HMAC-MD5-96
Autenticación	Contraseña

Activación del panel frontal para la conexión del iKVM

Para obtener información e instrucciones sobre el uso de los puertos del panel frontal de iKVM, consulte [Activación o desactivación del panel frontal](#).

Configuración del software de emulación de terminal

El CMC admite una consola de texto Telnet o serie de una estación de administración que ejecute uno de los siguientes tipos de software de emulación de terminal:

- 1 Linux Minicom en Xterm
- 1 HyperTerminal Private Edition (versión 6.3) de Hilgraeve
- 1 Linux Telnet o SSH en un Xterm
- 1 Microsoft® Telnet

Realice los pasos en los apartados siguientes para configurar el tipo del software de terminal. Si está usando Microsoft Telnet, no se requiere la configuración.

Configuración de Linux Minicom para la emulación de consola serie

Minicom es una 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 en [Valores de Minicom necesarios para la emulación de consola serie](#) para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0 para emulación de la consola serie

 **NOTA:** Para garantizar que el texto se muestre correctamente, Dell recomienda que se utilice una ventana de Xterm para mostrar la consola Telnet en vez de la consola predeterminada que ofrece la instalación de Linux.

1. Para iniciar una nueva sesión de Xterm, escriba `xterm &` en la petición de comandos.
2. En la ventana de Xterm, lleve la flecha del mouse a la esquina inferior derecha de la ventana y cambie el tamaño de la ventana a 80 x 25.
3. Si no tiene un archivo de configuración de Minicom, vaya al siguiente paso.
Si tiene un archivo de configuración de Minicom, escriba `minicom <nombre de archivo de configuración de Minicom>` y prosiga al paso 17.
4. En la petición de comandos de Xterm, escriba `minicom -s`.
5. Seleccione **Serial Port Setup (Configuración de puerto serie)** y pulse <Intro>.
6. Presione <a> y seleccione el dispositivo serie adecuado (por ejemplo, `/dev/ttyS0`).
7. Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
8. Presione <f> y luego defina la opción **Control de flujo de hardware** en **Sí** y la opción **Control de flujo de software** en **No**.
Para salir del menú **Configuración del puerto serie**, presione <Entrar>.
9. Seleccione **Módem y marcación** y presione <Entrar>.
10. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **restablecer**, **conectar** y **colgar** de modo que queden en blanco.
11. Presione <Entrar> para guardar cada uno de los valores en blanco.
12. Cuando se hayan borrado todos los campos especificados, presione <Entrar> para salir del menú **Configuración de parámetros y marcación de módem**.
13. Seleccione **Guardar configuración como nombre_de_config** y presione <Entrar>.
14. Seleccione **Salir de Minicom** y presione <Entrar>.
15. Cuando el sistema solicite un shell de comandos, escriba `minicom <nombre de archivo de configuración de Minicom>`.
Para ampliar la ventana de Minicom a 80 x 25, arrastre la esquina de la misma.
16. Presione <Ctrl+a>, <z>, <x> para salir de Minicom.

Asegúrese que la ventana de Minicom muestre una petición de comandos, por ejemplo, `[iDRAC\root]#`. Cuando la petición de comandos aparezca, la conexión se habrá establecido satisfactoriamente y usted estará listo para conectarse a la consola del sistema administrado por medio del comando `serie connect`.

Valores de Minicom necesarios para la emulación de consola serie

Utilice la [tabla 3-3](#) para configurar cualquier versión de Minicom.

Tabla 3-3. Valores de Minicom para emulación de consola serie

Descripción del valor	Valor necesario
Bps/Par/Bits	115200 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Marcación de módem y configuración de parámetros	Borre los valores init , restablecer , conectar y colgar de modo que queden en blanco
Tamaño de ventana	80 x 25 (para cambiar el tamaño, arrastre la esquina de la ventana)

Ejecución de Telnet con Windows XP o Windows 2003

Si la estación de administración ejecuta Windows XP o Windows 2003, pueden presentarse problemas de caracteres en una sesión Telnet del CMC. El problema puede consistir en un inicio de sesión bloqueado en el que la tecla <Entrar> no responde y no aparece la solicitud para ingresar la contraseña.

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

Configuración de Linux para la redirección de la consola serie del servidor durante el inicio

Los pasos a continuación son específicos para GRand Unified Bootloader (GRUB) de Linux. Cambios similares serían necesarios si se usa un cargador de inicio diferente.

 **NOTA:** Cuando configure la ventana de emulación de cliente VT100, configure la ventana o aplicación que esté mostrando la consola redirigida en 25 filas x 80 columnas a fin de garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo `/etc/grub.conf` como se indica a continuación:

1. Localice las secciones de configuración general en el archivo y agregue las siguientes dos líneas nuevas:

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. Agregue dos opciones a la línea de núcleo:

```
kernel..... console=ttyS1,57600
```

3. Si el archivo `/etc/grub.conf` contiene una directiva `splashimage`, inserte un carácter de comentario al inicio de la línea para anularla.

El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE: You do not have a /boot partition. This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
  root (hd0,0)
  kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/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 (hd0,0)
  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`, aplique las siguientes directrices:

1. Desactive la interfaz gráfica de GRUB y utilice la interfaz de texto. De lo contrario, la pantalla de GRUB no se mostrará en la redirección de la consola. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con `splashimage`.
1. Para abrir varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión serie, agregue la siguiente línea a todas las opciones:

```
console=ttyS1,57600
```

El ejemplo muestra el elemento `console=ttyS1,57600` agregado sólo a la primera opción.

Activación del inicio de sesión en la consola serie del servidor después de inicio

Modifique el archivo `/etc/inittab`, como se indica a continuación:

1. Agregue una nueva línea para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

El siguiente ejemplo muestra el archivo con la nueva línea.

```

#
# inittab This file describes how the INIT process
#         should set up the system in a certain
#         run-level.
#
# Author: Miquel van Smoorenburg
#         Modified for RHS Linux by Marc Ewing and
#         Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you
#    do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

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.
ud:once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon

```

Modifique el archivo `/etc/securetty`, como se indica a continuación:

- 1 Agregue una nueva línea, con el nombre del tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

```

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

```

Conexión a módulos por medio del comando connect

Durante una conexión de línea de comandos, el CMC permite que el comando `connect` establezca una conexión serie con módulos de E/S y de servidor. La conexión a los módulos de servidor sólo se ofrece para fines de depuración de errores del sistema operativo. Para conectarse a módulos de servidor y utilizar las consolas remotas del sistema operativo, debe utilizar la función de redirección de consola de la interfaz web de iDRAC o la función de comunicación en serie en LAN (SOL) del iDRAC.

-  **AVISO:** Cuando se ejecuta desde la consola serie del CMC, la opción `connect -b` permanece conectada hasta que se restablece el CMC. Esta conexión es un riesgo potencial de seguridad.
-  **NOTA:** El comando `connect` ofrece la opción `-b` (binario). Esta opción transmite datos binarios sin procesar y no utiliza `cfgSerialConsoleQuitKey`. Además, al establecer conexión con un servidor por medio de la consola serie del CMC, las transiciones en la señal DTR (por ejemplo, si el cable serie se retira para conectar un depurador de errores) no causan una desconexión.
-  **NOTA:** Si un módulo de E/S no admite la redirección de consola, el comando `connect` mostrará una consola vacía. En tal caso, para regresar a la consola del CMC escriba la secuencia de escape. La secuencia de escape predeterminada para la consola es `<Ctrl>\`.

Existen hasta seis módulos de E/S en el sistema administrado. Para conectarse a un módulo de E/S escriba:

```
connect switch-n
```

donde *n* es una etiqueta del módulo de E/S a1, a2, b1, b2, c1 y c2.

Los módulos de E/S llevan las etiquetas A1, A2, B1, B2, C1 y C2 (Consulte tabla 10-1 para obtener una ilustración de la colocación de los módulos de E/S en el chasis). Cuando hace referencia a los módulos de E/S en el comando `connect`, los módulos de E/S se asignan a conmutadores como se muestra en [tabla 3-4](#).

Tabla 3-4. Asignación de módulos de E/S a conmutadores

Etiqueta del módulo de E/S	Conmutador
A1	conmutador-a1
A2	conmutador-a2
B1	conmutador-b1
B2	conmutador-b2
C1	conmutador-c1
C2	conmutador-c2

-  **NOTA:** Sólo puede haber una conexión de módulo de E/S por chasis al mismo tiempo.
-  **NOTA:** No es posible establecer conexiones de paso desde la consola serie.

Para conectarse a un servidor administrado para efectuar la depuración de errores, utilice el comando `connect server-n`, donde *-n* representa el número de ranura del servidor que se desea depurar. Al establecer conexión con un servidor, se asume la existencia de una comunicación binaria y el carácter de escape se deshabilita. Si iDRAC no se encuentra disponible, aparecerá el mensaje de error `No existe ruta al host`. Asegúrese que el servidor está insertado correctamente y que el iDRAC tuvo suficiente tiempo para completar la rutina de inicio.

Para obtener información sobre cómo conectarse a través de una conexión serie, consulte [Configuración del CMC para el uso de consolas de línea de comandos](#).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Glosario

Guía del usuario

Active Directory

Active Directory es un sistema centralizado y estandarizado que automatiza la administración de red de los datos de usuario, la seguridad y los recursos distribuidos y hace posible las operaciones con otros directorios. Active Directory está diseñado específicamente para los entornos de red distribuidos.

ARP

Protocolo para resolución de direcciones, un método para encontrar la dirección Ethernet de un host a partir de su dirección de Internet.

ASCII

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

BIOS

Sistema básico de entradas y salidas, la parte del software del sistema que proporciona la interfaz de menor nivel con los dispositivos periféricos y que controla la primera fase del proceso de inicio del sistema, incluso la instalación del sistema operativo en la memoria.

bus:

Conjunto de conductores que conectan las distintas unidades funcionales en un equipo. Los buses reciben su nombre en función del tipo de datos que llevan, por ejemplo, bus de datos, bus de direcciones o bus de PCI.

CA

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

captura SNMP

Notificación (suceso) generada por el CMC que contiene información sobre los cambios de estado en el sistema administrado o sobre problemas potenciales de hardware.

CD

Disco compacto

CLI

Interfaz de línea de comandos

CMC

Dell Chassis Management Controller, que ofrece funciones de administración remota y control de alimentación para los sistemas Dell PowerEdge™.

DHCP

Protocolo de configuración de host dinámica, un método para asignar dinámicamente direcciones IP a los equipos de una red.

Dirección MAC

Dirección de control de acceso a medios, una dirección única incorporada en los componentes físicos de una tarjeta de interfaz de red (NIC).

disco RAM

Programa residente en la memoria que emula una unidad de disco duro.

DLL

Biblioteca de vínculo dinámico, una biblioteca de funciones que pueden ser invocadas por un programa más grande que se ejecuta en el sistema de ser necesario. Los funciones menores permiten que el programa más grande se comunice con un dispositivo específico como una impresora o un escáner.

DNS

Sistema de nombres de dominio

esquema ampliado

Solución que se usa con Active Directory para determinar el acceso de los usuarios al CMC; utiliza objetos de Active Directory definidos por Dell.

esquema estándar

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

Estación de administración

Sistema que puede acceder de forma remota al CMC.

FQDN

Nombre de dominio completamente calificado, un nombre de dominio que especifica la posición absoluta de un módulo en la jerarquía de árbol de DNS. Microsoft® Active Directory® sólo admite FQDN de 64 bytes o menos.

FSMO

Operación de maestro único flexible, una tarea del controlador de dominio de Microsoft Active Directory que garantiza la atomicidad de una operación de extensión.

GB1

El puerto de enlace ascendente en el chasis.

GMT

Hora del meridiano de Greenwich. La GMT es la hora estándar utilizada en todo 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.

GUI

Interfaz gráfica del usuario, término que hace referencia a una interfaz de pantalla que usa elementos como ventanas, cuadros de diálogo y botones, en contraposición a una interfaz con petición de comandos en la que toda la interacción de los usuarios se muestra y se escribe en forma de texto.

hardware log

Registro generado por el CMC de los sucesos relacionados con el hardware en el chasis.

ICMP

Protocolo de mensajes de control en Internet, un método que permite a los sistemas operativos enviar mensajes de error.

ID

Identificador, término usado comúnmente para hacer referencia a la identificación de un usuario (Id. de usuario) o de un objeto (Id. de objeto).

IDRAC

Dell Integrated Remote Access Controller, hardware de administración de sistemas y solución de software que brinda funciones de administración remota, recuperación ante fallas del sistema y control de alimentación para los sistemas Dell PowerEdge.

IKVM

Módulo de conmutador KVM integrado Avocent®, un módulo opcional de acoplamiento activo al chasis que ofrece acceso local de teclado, mouse y vídeo a cualquiera de los 16 servidores del chasis, así como la opción adicional de consola del CMC de Dell que se conecta al CMC activo del chasis.

IOMINIF

Dispositivo de infraestructura del módulo de E/S.

IP

Protocolo de Internet. IP es la capa de red de TCP/IP. El IP proporciona enrutamiento, fragmentación y reensamblaje de paquetes.

IPMB

Bus de administración de plataforma inteligente, que se utiliza en la tecnología de administración de sistemas.

Kbps

Kilobits por segundo, una unidad de velocidad de transferencia de datos.

LAN

Red de área local

LDAP

Protocolo ligero de acceso a directorios

LED

Diodo emisor de luz

LOM

Red de área local en la placa base

MAC

Control de acceso a medios, un subnivel de red entre un nodo de red y el nivel físico de la red.

Mbps

Megabits por segundo, una unidad de velocidad de transferencia de datos.

MC

Tarjeta intermedia

Microsoft Active Directory

Sistema centralizado y estandarizado que automatiza la administración de red de datos de usuarios, seguridad y recursos distribuidos, y permite la operación con otros directorios. Active Directory está diseñado específicamente para los entornos de red distribuidos.

Módulo de alta densidad

Un servidor independiente diseñado para estantes de alta densidad.

NIC

Tarjeta de interfaz de red, una placa de circuito de adaptadores instalada en un equipo para brindar conexión física a una red.

OID

Identificador de objeto

OSCAR

Configuración y elaboración de informes en pantalla (On Screen Configuration and Reporting), una interfaz gráfica de usuario utilizada para acceder a iKVM.

PCI

Interconexión de componentes periféricos, tecnología de interfaz y bus estándar para la conexión de dispositivos periféricos a un sistema y su comunicación.

POST

Autopruueba de encendido, una secuencia de pruebas de diagnóstico ejecutadas automáticamente por un sistema al encenderse.

RAC

Controladora de acceso remoto

RAM

Memoria de acceso aleatorio. Es una memoria con diversos fines instalada en los sistemas que permite la lectura y la escritura.

ROM

Memoria de sólo lectura. Permite leer pero no escribir datos.

RPM

Red Hat Package Manager, sistema de administración de paquetes para el sistema operativo Red Hat Enterprise Linux. RPM administra la instalación de paquetes de software. Es similar a un programa de instalación.

SAI

Fuente de alimentación ininterrumpible

SEL

Registro de sucesos del sistema o registro de hardware

SMTP

Protocolo simple de transferencia de correo, utilizado para transferir mensajes de correo electrónico entre diversos sistemas, por lo general a través de una conexión Ethernet.

SNMP

Protocolo simple de administración de red, diseñado para administrar nodos en una red IP. Los iDRAC son dispositivos administrados por SNMP (nodos).

Solicitud de firma de certificado (CSR)

Solicitud digital que se hace a una autoridad de certificados a fin de obtener un certificado de servidor seguro.

SSH

Secure Shell, protocolo de red que permite el intercambio de datos entre dos equipos a través de un canal seguro.

SSL

Nivel de conexión segura (Secure Sockets Layer), protocolo que ofrece comunicaciones seguras a través de redes para la transferencia de datos.

STK

El puerto de demarcación en el chasis

TCP/IP

Protocolo de control de transmisiones/Protocolo de Internet que representan el conjunto de protocolos Ethernet estándar que incluyen los protocolos de nivel de red y transporte.

TFTP

Protocolo trivial de transferencia de archivos, un protocolo simple usado para descargar códigos de inicio a dispositivos o sistemas sin discos.

tiempo de retardo (interfaz de usuario de OSCAR)

La cantidad de segundos que transcurren antes de que el cuadro de diálogo principal de OSCAR aparezca al presionar <Imprimir pantalla>.

USB

Bus serie universal, un estándar para establecer conexión con dispositivos.

UTC

Hora coordinada universal. *Consulte* GMT.

vKVM

Consola virtual de teclado, vídeo y mouse

VLAN

Red de área local virtual

VNC

Informática de redes virtuales

VT-100

Video Terminal 100, una herramienta que utilizan los programas de emulación de terminal más comunes.

WAN

Red de área amplia

[Regresar a la página de contenido](#)

Guía del usuario

Notas y avisos

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

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

La información contenida en este documento puede modificarse sin previo aviso.
© 2008 Dell Inc. Todos los derechos reservados.

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

Marcas comerciales usadas en este texto: *Dell*, el logo de *DELL*, *OpenManage*, *PowerEdge* y *PowerConnect* son marcas comerciales de Dell Inc.; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT*, *Windows Server* y *Windows Vista* son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y en otros países; *Red Hat* y *Red Hat Enterprise Linux* son marcas comerciales registradas de Red Hat, Inc.; *Novell* y *SUSE* son marcas comerciales registradas de Novell Corporation en los Estados Unidos y en otros países; *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. *Avocent* es una marca comercial de Avocent Corporation; *OSCAR* es una marca comercial registrada de Avocent Corporation o de sus afiliados.

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo según lo autoriza la licencia pública de OpenLDAP. Hay una copia de esta licencia disponible en el archivo LICENSE en el directorio principal de la distribución o, como alternativa, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Hay archivos individuales y/o paquetes recibidos en contribuciones que pueden ser propiedad intelectual de terceros y están sujetos a restricciones adicionales. Este trabajo se deriva de la distribución LDAP v3.3 de la Universidad de Michigan. Este trabajo también contiene materiales que provienen de fuentes públicas. La información sobre OpenLDAP se puede obtener 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, siempre y cuando se conserve este aviso. Los nombres de los titulares de la propiedad intelectual no se deben usar para endosar o promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Se permite la redistribución y uso en formatos binario y original siempre y cuando se conserve este aviso y se conceda el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se debe usar para endosar ni promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas.

Es posible que se utilicen otros nombres y marcas comerciales en este documento para hacer referencia a las entidades que son dueñas de las marcas y nombres o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Agosto de 2008 Rev. A00

Notas y avisos

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

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

La información contenida en este documento puede modificarse sin previo aviso.
© 2008 Dell Inc. Todos los derechos reservados.

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

Marcas comerciales usadas en este texto: *Dell*, el logo de *DELL*, *OpenManage*, *PowerEdge* y *PowerConnect* son marcas comerciales de Dell Inc.; *Microsoft*, *Active Directory*, *Internet Explorer*, *Windows*, *Windows NT*, *Windows Server* y *Windows Vista* son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y en otros países; *Red Hat* y *Red Hat Enterprise Linux* son marcas comerciales registradas de Red Hat, Inc.; *Novell* y *SUSE* son marcas comerciales registradas de Novell Corporation en los Estados Unidos y en otros países; *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. *Avocent* es una marca comercial de Avocent Corporation; *OSCAR* es una marca comercial registrada de Avocent Corporation o de sus afiliados.

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo según lo autoriza la licencia pública de OpenLDAP. Hay una copia de esta licencia disponible en el archivo LICENSE en el directorio principal de la distribución o, como alternativa, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Hay archivos individuales y/o paquetes recibidos en contribuciones que pueden ser propiedad intelectual de terceros y están sujetos a restricciones adicionales. Este trabajo se deriva de la distribución LDAP v3.3 de la Universidad de Michigan. Este trabajo también contiene materiales que provienen de fuentes públicas. La información sobre OpenLDAP se puede obtener 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, sólo 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. All rights reserved. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, siempre y cuando se conserve este aviso. Los nombres de los titulares de la propiedad intelectual no se deben usar para endosar o promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas. Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. Se permite la redistribución y uso en formatos binario y original siempre y cuando se conserve este aviso y se conceda el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se debe usar para endosar ni promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas.

Es posible que se utilicen otros nombres y marcas comerciales en este documento para hacer referencia a las entidades que son dueñas de las marcas y nombres o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Agosto de 2008 Rev. A00

[Regresar a la página de contenido](#)

Uso de FlexAddress

Guía del usuario

- [Activar FlexAddress](#)
- [Desactivar FlexAddress](#)
- [Ver el estado de FlexAddress a través de la CLI](#)
- [Configurar FlexAddress a través de la CLI](#)
- [Encendido en LAN con FlexAddress](#)
- [Solución de problemas de FlexAddress](#)
- [CONTRATO DE LICENCIA DEL SOFTWARE de DELL FlexAddress](#)

La función FlexAddress es una actualización opcional presentada en CMC 1.1 que permite a los módulos del servidor reemplazar las identificaciones de red World Wide Name y Media Access Control (WWN/MAC) asignadas de fábrica con identificaciones WWN/MAC proporcionadas por el chasis.

Se asigna una identificación WWN y MAC única a cada módulo del servidor como parte del proceso de fabricación. Antes de FlexAddress, si tenía que reemplazar el módulo de un servidor por otro, las identificaciones WWN y MAC se cambiaban, y las herramientas de administración de red Ethernet y los recursos SAN debían configurarse nuevamente para dar cuenta del nuevo módulo del servidor.

FlexAddress permite al CMC asignar identificaciones WWN/MAC a una ranura particular e *invalidar* las identificaciones de fábrica. Si se reemplaza el módulo del servidor, las identificaciones WWN/MAC basadas en la ranura siguen siendo las mismas. Esta función elimina la necesidad de volver a configurar las herramientas de administración de red Ethernet y los recursos SAN para un nuevo módulo del servidor.

Además, la acción de *invalidar* sólo ocurre cuando un módulo del servidor se inserta en un chasis con FlexAddress activado; no se realizan cambios permanentes al módulo del servidor. Si un módulo del servidor se traslada a un chasis que no admite FlexAddress, se usarán las identificaciones WWN/MAC asignadas de fábrica.

Antes de instalar FlexAddress, puede determinar el rango de las direcciones MAC contenidas en una tarjeta de función de FlexAddress al insertar la tarjeta SD en una lectora de tarjetas de memoria USB y ver el archivo `pwwn_mac.xml`. Este archivo XML de texto claro en la tarjeta SD contendrá una etiqueta XML `mac_start` que es la primera dirección MAC hexadecimal de inicio que se usará para este rango único de direcciones MAC. La etiqueta `mac_count` es el número total de direcciones MAC que asigna la tarjeta SD. El rango MAC total asignado se puede determinar por:

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

Por ejemplo: (iniciar_mac)00188BFFDCFA + 0xCF = (cerrar_mac)00188BFFDDC9



NOTA: Debe bloquear la tarjeta SD antes de insertarla en la "Lectora de tarjetas de memoria" USB para evitar que se modifique el contenido por accidente. Debe **DESBLOQUEAR** la tarjeta SD antes de insertarla en el CMC.

Activar FlexAddress

FlexAddress se entrega en una tarjeta Secure Digital (SD) que debe insertarse en el CMC para proporcionar las identificaciones WWN/MAC asignadas por el chasis. Se requieren varias actualizaciones para activar la función FlexAddress; si **no planea activar FlexAddress, no son necesarias estas actualizaciones**. Las actualizaciones, que se muestran en la tabla a continuación, incluyen el BIOS de los módulos del servidor, el firmware o el BIOS de tarjetas intermedias de E/S y el firmware del CMC. Debe actualizar todos estos componentes antes de activar FlexAddress. Si no se aplican estas actualizaciones, la función FlexAddress no funcionará como se espera.

Componente	Versión mínima requerida
Tarjeta intermedia Ethernet: Broadcom M5708t	Firmware del código de inicio 4.4.1 o posterior Firmware de inicio iSCSI 2.7.11 o posterior Firmware PXE 4.4.3 o posterior
Tarjeta intermedia FC: QLogic QME2472	BIOS 2.04 o posterior
Tarjeta intermedia FC: Emulex LPe1105-M4	BIOS 3.03a3 y firmware 2.72A2 o posterior
BIOS del módulo del servidor	BIOS 2.02 (PowerEdge™ M600) o posterior BIOS 2.03 (PowerEdge M605) o posterior
PowerEdgeM600/M605 LAN en placa base (LOM)	Firmware del código de inicio 4.4.1 o posterior Firmware de inicio iSCSI 2.7.11 o posterior
iDRAC	Versión 1.11 o posterior
CMC	Versión 1.11 o posterior

Para asegurar la instalación correcta de la función FlexAddress, actualice el BIOS y el firmware en este orden:

1. Actualice el firmware y el BIOS de todas las tarjetas intermedias.
2. Actualice el BIOS del módulo del servidor.
3. Actualice el firmware del iDRAC en el módulo del servidor.
4. Actualice el firmware de todos los CMC en el chasis; si hay CMC redundantes, asegúrese de que ambos estén actualizados.

5. En un sistema redundante de módulos CMC, inserte la tarjeta SD en el módulo pasivo o en el módulo CMC individual para un sistema no redundante.

 **NOTA:** Si el firmware del CMC que admite FlexAddress (versión 1.10 o posterior) no está instalado, no se activará la función.

Consulte el documento *Especificaciones técnicas de IChassis Management Controller (CMC) Secure Digital (SD) Card* para obtener instrucciones de instalación de la tarjeta SD.

 **NOTA:** La tarjeta SD contiene la función FlexAddress. La información contenida en la tarjeta SD está cifrada y no es posible duplicarla o alterarla de ninguna forma porque podría desactivar las funciones del sistema y ocasionar que el sistema deje de funcionar.

 **NOTA:** El uso de la tarjeta SD está limitado a un sólo chasis. Si tiene más de un chasis debe adquirir tarjetas SD adicionales.

La activación de la función FlexAddress es automática cuando se reinicia el CMC con la tarjeta de función SD instalada; esta activación hará que la función se adhiera al chasis actual. Si tiene la tarjeta SD instalada en el sistema CMC redundante, la activación de la función FlexAddress no se producirá hasta que se active el CMC redundante. Consulte el documento *Especificaciones técnicas de Chassis Management Controller (CMC) Secure Digital (SD) Card* para obtener información sobre cómo activar un CMC redundante.

Cuando reinicia el CMC, verifique el proceso de activación siguiendo los pasos de la próxima sección, "[Verificar la activación de FlexAddress](#)".

Verificar la activación de FlexAddress

Para asegurar la activación adecuada de FlexAddress, se pueden usar los comandos de RACADM para verificar la tarjeta de función SD y la activación de FlexAddress.

Use el siguiente comando de RACADM para verificar la tarjeta de función SD y su estado:

```
racadm featurecard -s
```

La siguiente tabla enumera los mensajes de estado que muestra el comando.

Tabla 6-1. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
No se insertó ninguna tarjeta de función.	Controle el CMC para verificar que la tarjeta SD se insertó correctamente. En una configuración de CMC redundante, asegúrese de que el CMC con la tarjeta de función SD instalada sea el CMC activo y no el CMC en espera.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está sujeta a este chasis.	No es necesaria ninguna acción.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está sujeta a otro chasis. svctag = ABC1234, tarjeta SD SN = 01122334455	Retire la tarjeta SD; coloque e instale la tarjeta SD en el chasis actual.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función no está sujeta a ningún chasis.	La tarjeta de función se puede mover a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, ingrese racadm racreset hasta que se active el módulo del CMC con la tarjeta de función instalada.

Utilice el siguiente comando de RACADM para mostrar todas las funciones activadas en el chasis:

```
racadm feature -s
```

Este comando mostrará el siguiente mensaje de estado:

```
Feature = FlexAddress
```

```
Date Activated = 8 April 2008 - 10:39:40
```

```
Feature installed from SD-card SN = 01122334455
```

```
(Función = FlexAddress
```

```
Fecha de activación = 8 de abril de 2008 - 10:39:40
```

```
Función instalada desde la tarjeta SD SN = 01122334455)
```

Si no hay funciones activadas en el chasis, el comando mostrará un mensaje:

```
racadm feature -s
```

```
No features active on the chassis.
```

```
(No hay funciones activadas en el chasis.)
```

Después de ejecutar los dos comandos, se verifica la activación de la función FlexAddress. Para obtener más información sobre los comandos de RACADM, consulte [feature](#) y [tarjeta de función](#).

Desactivar FlexAddress

La función FlexAddress se puede desactivar y la tarjeta SD se puede regresar a un estado previo a la instalación a través de un comando de RACADM. No hay ninguna función de desactivación en la interfaz web. La desactivación regresará la tarjeta SD a su estado original, en el que se la puede instalar y activar en un chasis diferente.

 **AVISO:** La tarjeta SD debe estar instalada físicamente en el CMC, y el chasis debe estar apagado antes de ejecutar el comando de desactivación o se podría producir una pérdida de datos.

Si ejecuta el comando de desactivación sin que haya una tarjeta instalada, o con una tarjeta de un chasis diferente, la función se desactivará y no se realizará ningún cambio a la tarjeta.

Desactivar FlexAddress

Use el siguiente comando de RACADM para desactivar la función FlexAddress y restaurar la tarjeta SD:

```
racadm feature -d -c flexaddress
```

El comando mostrará el siguiente mensaje de estado luego de la desactivación satisfactoria:

```
feature FlexAddress is deactivated on the chassis successfully.
```

(La función FlexAddress se ha desactivado en el chasis satisfactoriamente.)

Si el chasis no se apaga antes de la ejecución, el comando mostrará el siguiente mensaje de error:

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

(ERROR: no se puede desactivar la función porque el chasis está encendido)

Para obtener más información sobre el comando, consulte [feature](#).

Ver el estado de FlexAddress a través de la CLI

Puede usar la interfaz de línea de comandos para ver información del estado de FlexAddress. Puede ver información del estado del chasis completo o de una ranura particular. La información que se muestra incluye:

- 1 Configuración de la estructura de red
- 1 FlexAddress activado/desactivado
- 1 Número y nombre de la ranura
- 1 Direcciones asignadas por el chasis y por el servidor
- 1 Direcciones en uso

Use el siguiente comando de RACADM para mostrar el estado de FlexAddress para todo el chasis:

```
racadm getflexaddr
```

Para mostrar el estado de FlexAddress para una ranura particular:

```
racadm getflexaddr [-i <N° ranura>]
```

<N° ranura> = 1 a 16

Consulte "Configurar FlexAddress" para obtener detalles adicionales sobre la configuración de FlexAddress. Para obtener información adicional sobre el comando, consulte [getflexaddr](#).

Configurar FlexAddress a través de la CLI

Puede utilizar la interfaz de línea de comandos para activar o desactivar FlexAddress por estructura de red. Además, puede activar/desactivar la función por ranura. Después de haber activado la función por estructura de red, puede seleccionar las ranuras que se activarán. Por ejemplo, si Estructura de red A está activada, todas las ranuras activadas tendrán FlexAddress activado sólo en la Estructura de red A. El resto de las estructuras de red usarán la WWN/MAC asignada por la fábrica en el servidor.

Las ranuras activadas tendrán FlexAddress activado para todas las estructuras de red activadas. Por ejemplo, no es posible activar la Estructura de red A y B y tener la Ranura 1 con FlexAddress activado en la Estructura de red A pero no en la Estructura de red B.

Use el siguiente comando de RACADM para activar o desactivar estructuras de red:

```
racadm setflexaddr [-f <nombre de estructura de red> <estado>]
```

<nombre de estructura de red> = A, B, C

<estado> = 0 o 1

Donde **0** es desactivar y **1** es activar.

Use el siguiente comando de RACADM para activar o desactivar ranuras:

```
racadm setflexaddr [-i <N° ranura> <estado>]
```

<N° ranura> = 1 a 16

<estado> = 0 o 1

Donde **0** es desactivar y **1** es activar.

Para obtener información adicional sobre el comando, consulte [setflexaddr](#).

Configuración adicional de FlexAddress para Linux

Cuando se cambia de una identificación MAC asignada por el servidor a una identificación MAC asignada por el chasis en sistemas operativos basados en Linux, es posible que se requieran pasos adicionales de configuración:

- 1 SLES 9 y SLES 10: es posible que los usuarios necesiten ejecutar YAST (Yet another Setup Tool) en el sistema Linux para configurar los dispositivos de red y luego reiniciar los servicios de red.
- 1 Red Hat® Enterprise Linux® 4(RHEL) y RHEL 5: los usuarios necesitarán ejecutar Kudzu, una utilidad para detectar y configurar hardware nuevo/cambiado en el sistema. Kudzu le presentará al usuario The Hardware Discovery Menu, que detectará el cambio de la dirección MAC como un retiro de hardware y una incorporación de hardware nuevo.

Encendido en LAN con FlexAddress

Cuando se instala la función FlexAddress por primera vez en un módulo del servidor, se requiere una secuencia de apagado y encendido para que FlexAddress se active. FlexAddress en dispositivos Ethernet se programa por el BIOS del módulo del servidor. Para que el BIOS del módulo del servidor programe la dirección, necesita estar en funcionamiento, lo que requiere que el módulo del servidor se encienda. Cuando se completan las secuencias de apagado y encendido, las identificaciones MAC asignadas por el chasis están disponibles para la función Encendido en LAN (WOL).

Solución de problemas de FlexAddress

Esta sección contiene información de solución de problemas para FlexAddress.

1. ¿Qué sucede si se retira una tarjeta de función?

Nada. Las tarjetas de función se pueden retirar y almacenar o se pueden dejar en el lugar.

2. ¿Qué sucede si se retira una tarjeta de función que se usó en un chasis y se coloca en otro?

La interfaz web mostrará un error que dice:

```
This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

(Esta tarjeta de función se activó con otro chasis. Debe retirarse antes de acceder a la función FlexAddress.)

```
Etiqueta de servicio del chasis actual = XXXXXXXX
```

```
Etiqueta de servicio del chasis de tarjeta de función = YYYYYYYY)
```

Todas las anotaciones serán agregadas al registro del CMC que dice:

```
cmc <date timestamp> : feature 'FlexAddress@XXXXXXX' not activated; chassis ID='YYYYYYY'
```

```
(cmc <fecha y hora> : función 'FlexAddress@XXXXXXX' no activado; ID de chasis='YYYYYYY')
```

3. ¿Qué sucede si se retira la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

La tarjeta no debería activarse ni sufrir modificaciones. El CMC ignorará esta tarjeta. En esta situación, el `$racadm featurecard -s` mostrará un mensaje:

```
No feature card inserted
```

```
ERROR: can't open file
```

(No se insertó ninguna tarjeta de función)

ERROR: no se puede abrir archivo)

4. Si se reprograma la etiqueta de servicio del chasis, ¿qué sucede si hay una tarjeta de función sujeta a ese chasis?

La interfaz web mostrará un error que dice:

This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.

Current Chassis Service Tag = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

(Esta tarjeta de función se activó con otro chasis. Debe retirarse antes de acceder a la función FlexAddress.

Etiqueta de servicio del chasis actual = XXXXXXXX

Etiqueta de servicio del chasis de tarjeta de función = YYYYYYYY)

Dell Service necesitará programar nuevamente la etiqueta de servicio del chasis original en el chasis y reiniciar el CMC.

5. ¿Qué sucede si tengo dos tarjetas de función instaladas en el sistema CMC redundante? ¿recibiré un error?

La tarjeta de función en el CMC activo estará activada e instalada en el chasis. El CMC ignorará la segunda tarjeta.

6. ¿La tarjeta SD tiene un bloqueo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo CMC, verifique que el pestillo de protección contra escritura esté en la posición desbloqueada. No se puede activar la función FlexAddress si la tarjeta SD está protegida contra escritura. En esta situación, el comando `$racadm feature -s` mostrará este mensaje:

No features active on the chassis. ERROR: read only file system

(No hay funciones activadas en el chasis. ERROR: sistema de archivos de sólo lectura)

7. ¿Qué sucede si no hay una tarjeta SD en el módulo CMC activado?

El comando `$racadm featurecard -s` mostrará este mensaje:

No feature card inserted.

(No se insertó ninguna tarjeta de función.)

8. ¿Qué le sucederá a la función FlexAddress si el BIOS del servidor se actualiza de la versión 1.xx a la versión 2.xx?

Se debe apagar el módulo del servidor antes de que pueda usarse con FlexAddress. Después de que se completa la actualización del BIOS del servidor, el módulo del servidor no obtendrá direcciones asignadas por el chasis hasta que se realice un ciclo de encendido en el servidor.

9. ¿Qué sucede si un chasis con un sólo CMC está desactualizado con un firmware anterior a 1.10?

Se retirará la configuración y la función FlexAddress. Después de que se actualiza el firmware del CMC a 1.10 o superior, la función FlexAddress necesita que el usuario la reactive y la configure.

10. En un chasis con CMC redundantes, si se está reemplazando una unidad del CMC con una que tiene firmware anterior a 1.10, se debe utilizar el siguiente procedimiento para asegurar que NO se retire la configuración y la función FlexAddress actual.

- Asegúrese de que la versión del firmware del CMC activado sea siempre 1.10 o superior.
- Retire el CMC en espera e inserte el nuevo CMC en su lugar.
- Desde el CMC activado, actualice el firmware del CMC en espera a 1.10 o superior.

 **NOTA:** Si el usuario no actualiza el firmware del CMC en espera a 1.10 o superior y se produce una transferencia de funciones ante fallas, la función FlexAddress no estará configurada y el usuario deberá reactivar la función.

11. La tarjeta SD está instalada correctamente al igual que todas las actualizaciones de firmware/software. Veo que FlexAddress está activado, pero no puedo ver nada en la pantalla de utilización del servidor para usarlo ¿Cuál es el problema?

Éste es un problema de almacenamiento en caché del explorador; cierre el explorador y vuelva a abrirlo.

Mensajes de comando: la siguiente tabla muestra los comandos de RACADM y la salida de situaciones comunes de FlexAddress.

Tabla 6-2. Comandos y salida de FlexAddress

Situación	Comando	Salida
La tarjeta SD en el módulo CMC activado está sujeta a otra etiqueta de	<code>\$racadm featurecard -s</code>	The feature card inserted is valid and

servicio.		contains the following feature(s) FlexAddress: The feature card is bound to another chassis, svctag = J310TF1 SD card SN =0188BFFE03A (La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: la tarjeta de función está sujeta a otro chasis, svctag = J310TF1 tarjeta SD SN =0188BFFE03A)
La tarjeta SD en el módulo CMC activado está sujeta a la misma etiqueta de servicio.	\$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis (La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: la tarjeta de función está sujeta a este chasis)
La tarjeta SD en el módulo CMC activado no está sujeta a ninguna etiqueta de servicio.	\$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis (La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: la tarjeta de función no está sujeta a ningún chasis)
Función FlexAddress no activada en el chasis por cualquier razón (ninguna tarjeta SD insertada/ tarjeta SD dañada/ después de función desactivada/ tarjeta SD sujeta a un chasis diferente)	\$racadm setflexaddr [-f <nombre de estructura de red> <estado de ranura>] o \$racadm setflexaddr [-i N° ranura] <estado de ranura>]	ERROR: Flexaddress feature is not active on the chassis (ERROR: la función Flexaddress no está activada en el chasis)
Usuario invitado intenta configurar FlexAddress en ranuras/estructuras de red	\$racadm setflexaddr [-f <nombre de estructura de red> <estado de ranura>] \$racadm setflexaddr [-i N° ranura] <estado de ranura>]	ERROR: Insufficient user privileges to perform operation (ERROR: privilegios de usuario insuficientes para realizar la operación)
Desactivar la función FlexAddress con el chasis encendido	\$racadm feature -d -c flexaddress	ERROR: Unable to deactivate the feature because the chassis is powered ON (ERROR: no se puede desactivar la función porque el chasis está encendido)
Usuario invitado intenta desactivar la función en el chasis	\$racadm feature -d -c flexaddress	ERROR: Insufficient user privileges to perform operation (ERROR: privilegios de usuario insuficientes para realizar la operación)
Cambiar la configuración de FlexAddress de ranuras/estructuras de red mientras los módulos del servidor están encendidos	\$racadm setflexaddr -i 1 1 1	ERROR: Unable to perform the set operation because it affects a powered ON server (ERROR: no se puede realizar la operación de conjunto porque afecta a un servidor encendido)

CONTRATO DE LICENCIA DEL SOFTWARE de DELL FlexAddress

El presente documento es un contrato legal entre usted, el usuario y Dell Products, L.P. o Dell Global B.V. ("Dell"). Este contrato cubre todo el software que se distribuye con el producto Dell, para el que no existe un contrato de licencia diferente entre usted y el fabricante o el propietario del software (colectivamente, el "Software"). Este contrato no es para la venta de Software o de cualquier otra propiedad intelectual. Todos los derechos de título y propiedad intelectual en el Software y para éste pertenecen al fabricante o propietario del Software. Todos los derechos no otorgados expresamente bajo este contrato son derechos reservados por el fabricante o propietario del Software. Al abrir o romper el sello de los paquetes de Software, instalar o descargar el Software, o utilizar el Software que se ha cargado previamente o que se incluye en su producto, usted acepta estar sujeto a los términos de este contrato. Si no acepta estos términos, devuelva de inmediato todos los artículos de Software (discos, material escrito y embalaje) y suprima el Software cargado previamente o incluido en el producto.

Únicamente podrá utilizar una copia de Software por ordenador a la vez. Si dispone de varias licencias de Software, podrá utilizar en cualquier momento tantas copias como licencias tenga. Con el término "utilizar" se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del ordenador. La instalación en un servidor de red únicamente para la distribución a otros ordenadores no es "utilizar" si (y solo si) usted dispone de una licencia diferente para cada ordenador en el que se haya distribuido el Software. Debe asegurarse de que el número de personas que utilicen el Software instalado en un servidor de red no sea superior al número de licencias de las que disponga. Si el número de usuarios del Software instalado en un servidor de red supera el número de licencias, deberá adquirir licencias adicionales hasta que tenga el mismo número de licencias que de usuarios, antes de que éstos utilicen el Software. Si usted es un cliente comercial de Dell o un socio de Dell, por la presente concede a Dell, o a un representante seleccionado por Dell, el derecho a realizar una auditoría sobre el uso que usted hace del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y

proporcionarle todos los informes relacionados razonablemente con el uso que usted hace del Software. La auditoría se limitará a la verificación del cumplimiento de los términos de este contrato por su parte.

El Software está protegido por las leyes de copyright de Estados Unidos y por los tratados internacionales. Únicamente podrá hacer una copia del Software para disponer de una copia de respaldo o para archivarlo o transferirlo a un único disco duro, siempre que guarde el original sólo para disponer de una copia de respaldo o para archivarlo. No puede alquilar el software ni copiar los materiales impresos que se adjuntan con el mismo, pero sí puede transferir el software y todos los materiales adjuntos de manera permanente como parte de la venta o transferencia del producto Dell siempre y cuando no se quede con ninguna copia y los destinatarios acepten los términos de este documento. Cualquier transferencia deberá incluir la actualización más reciente y todas las versiones anteriores. No se permite retocar la ingeniería, descompilar o desmontar el Software. Si el paquete que acompaña a su ordenador contiene CD, disquetes de 3,5 pulgadas o de 5,25 pulgadas, podrá utilizar únicamente los adecuados para su ordenador. No podrá utilizar los discos en otro ordenador o red, ni prestarlos, alquilarlos, arrendarlos o transferirlos a otro usuario excepto tal y como lo permite el presente contrato.

GARANTÍA LIMITADA

Dell garantiza que los disquetes de Software no presentarán defectos en los materiales ni en su fabricación, siempre que se realice un uso normal, durante noventa (90) días, desde la fecha de recepción. Esta garantía se limita a usted y no es transferible. Las garantías implícitas se limitan a noventa (90) días desde la fecha de recepción del Software. En algunas jurisdicciones no existen limitaciones en la vigencia de la garantía implícita, de modo que esta limitación puede no ser aplicable en su caso. La responsabilidad total de Dell y de sus proveedores, así como su solución exclusiva, se limitará (a) a la devolución del importe pagado por el Software o (b) a la sustitución de cualquier CD o disquete que no cumpla esta garantía y que usted envíe a Dell con un número de autorización, por su cuenta y riesgo. Esta garantía limitada se anulará si se daña el disquete como resultado de un accidente, abuso, aplicación no adecuada, mantenimiento o modificación por parte de alguna persona que no pertenezca a Dell. La garantía cubre los disquetes sustituidos durante el período restante de la garantía original o durante treinta (30) días, dependiendo del plazo que sea mayor.

Dell NO garantiza que las funciones del Software satisfagan sus necesidades o que el funcionamiento del Software no se interrumpa o no tenga errores. Usted asume la responsabilidad de seleccionar el Software para lograr los resultados que espera, así como para utilizar los resultados obtenidos con el Software.

DELL, EN SU NOMBRE Y EN EL DE SUS PROVEEDORES, RENUNCIA AL RESTO DE GARANTÍAS, EXPLÍCITAS O IMPLÍCITAS, INCLUIDAS, PERO NO LIMITADAS A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR, POR LO QUE SE REFIERE AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS QUE LO ACOMPAÑAN. Esta garantía limitada le otorga derechos legales específicos, aunque puede disfrutar de otros, que varían en función de la jurisdicción.

EN NINGÚN CASO DELL O SUS PROVEEDORES SERÁN LOS RESPONSABLES DE LOS DAÑOS QUE PUEDAN OCURRIR (INCLUIDOS, SIN LIMITACIÓN, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, INTERRUPTIÓN O PÉRDIDA DE INFORMACIÓN DEL NEGOCIO O CUALQUIER OTRA PÉRDIDA PECUNIARIA) A CAUSA DEL USO O LA INCAPACIDAD DE UTILIZAR EL SOFTWARE, AUNQUE SE NOTIFIQUE LA POSIBILIDAD DE TALES DAÑOS. Puesto que algunas jurisdicciones no permiten la exclusión o limitación de responsabilidad por daños resultantes o accidentales, la limitación anteriormente mencionada puede no ser aplicable en su caso.

SOFTWARE FUENTE ABIERTO

Una parte de este CD puede contener software fuente abierto, que usted puede utilizar bajo los términos y condiciones de la licencia específica bajo la cual el software se distribuye.

ESTE SOFTWARE FUENTE ABIERTO SE DISTRIBUYE CON LA ESPERANZA DE QUE PUEDA SER ÚTIL, PERO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA EXPLÍCITA O EXPRESA; INCLUIDA PERO SIN LIMITARSE A LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR. BAJO NINGUNA CIRCUNSTANCIA SE HARÁN DELL, LOS POSEEDORES DEL COPYRIGHT O LOS CONTRIBUYENTES RESPONSABLES DE DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES, EJEMPLARES O CONSECUENTES (INCLUIDO, PERO SIN LIMITARSE A, LA ADQUISICIÓN DE SERVICIOS O PRODUCTOS SUSTITUIDOS; PÉRDIDA DE USO, DATOS O BENEFICIOS; O INTERRUPTIÓN COMERCIAL) SIN IMPORTAR LA MANERA EN QUE SE HAYAN PRODUCIDO NI LA TEORÍA DE RESPONSABILIDAD, YA SEA BAJO CONTRATO, RESPONSABILIDAD ESTRICTA O DELICTIVA (INCLUIDA LA NEGLIGENCIA O SIMILAR) QUE SE HAYAN OCASIONADO POR EL USO DE ESTE SOFTWARE, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE DICHO DAÑO.

DERECHOS LIMITADOS DEL GOBIERNO DE EE.UU.

El software y la documentación son "artículos comerciales" tal como se define dicho término en 48 C.F.R. 2.101, consiste de "software informático comercial" y "documentación de software informático comercial" como se utilizan dichos términos en 48 C.F.R. 12.212. Coherente con 48 C.F.R. 12.212 y 48 C.F.R. 227.7202-1 a 227.7202-4, todo EE.UU. Los usuarios finales gubernamentales adquieren el software y la documentación únicamente con los derechos estipulados en este documento. El contratante/fabricante es Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

GENERAL

Esta licencia estará en vigor hasta que finalice. Dicha finalización se llevará a cabo según las condiciones estipuladas anteriormente o si no cumple alguno de estos términos. Una vez haya finalizado, usted acepta que se destruya el Software y los materiales que lo acompañan, así como todas las copias de los mismos. Este contrato está regulado por las leyes del estado de Tejas. Las cláusulas de este contrato son independientes. Si se considera que alguna cláusula no es aplicable, el descubrimiento de este hecho no afectará la aplicabilidad del resto de las cláusulas, los términos o las condiciones de este contrato. Este contrato es vinculante para los sucesores y cesionarios. Tanto Dell como usted aceptan renunciar, según lo máximo permitido por la ley, a cualquier derecho a un proceso con jurado con respecto al Software o a este contrato. Puede que esta anulación no sea aplicable en su caso, por no ser efectiva en algunas jurisdicciones. Usted reconoce que ha leído el presente contrato, que lo entiende y acepta estar sujeto a sus términos, y que ésta es la declaración completa y exclusiva del contrato entre usted y Dell relativo al Software.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso del módulo iKVM

Guía del usuario

- [Información general](#)
 - [Interfaces de conexión física](#)
 - [Uso de OSCAR](#)
 - [Administración de servidores con iKVM](#)
 - [Administración del iKVM desde el CMC](#)
 - [Solución de problemas](#)
-

Información general

El módulo KVM de acceso local del chasis de servidor Dell™ M1000e se denomina módulo de conmutador KVM integrado Avocent® o iKVM. El módulo iKVM es un conmutador analógico de teclado, vídeo y mouse que se conecta en el chasis. Este módulo opcional de acoplamiento activo al chasis ofrece acceso local de teclado, mouse y vídeo a los servidores del chasis y la línea de comandos del CMC activo.

Interfaz de usuario del iKVM

El módulo iKVM utiliza la interfaz gráfica de usuario OSCAR® (On Screen Configuration and Reporting), que se activa mediante una tecla de acceso directo. OSCAR permite seleccionar uno de los servidores o la línea de comandos de Dell CMC a los que se desea acceder por medio del teclado, la pantalla y el mouse locales.

Sólo se permite una sesión de iKVM por chasis.

Seguridad

La interfaz de usuario OSCAR permite proteger el sistema por medio de una contraseña de protector de pantalla. Después de un período definido por el usuario, se inicia el modo de protección de pantalla y se prohíbe el acceso mientras no se introduzca la contraseña adecuada para reactivar OSCAR.

Exploración

OSCAR le permite seleccionar una lista de servidores, que aparecen en el orden en el que fueron seleccionados mientras OSCAR se encuentra en el modo de exploración.

Identificación de servidores

El CMC asigna nombres de ranuras a todos los servidores del chasis. Si bien el usuario puede asignar nombres a los servidores por medio de la interfaz OSCAR desde una conexión de niveles, los nombres asignados por el CMC tienen prioridad, por lo que los nombres nuevos asignados mediante OSCAR se sobrescribirán.

El CMC le asigna un nombre exclusivo a cada ranura para identificarla. Para modificar los nombres de las ranuras por medio de la interfaz web del CMC, consulte [Edición de los nombres de ranuras](#). Para modificar un nombre de ranura por medio de RACADM, consulte [setslotname](#).

Vídeo

Las conexiones de vídeo del iKVM admiten resoluciones de pantalla de entre 640 x 480 a 60 Hz y 1280 x 1024 a 60 Hz.

Plug and Play

El módulo iKVM admite el uso de la función Plug and Play de canal de datos para la pantalla (DDC), que automatiza la configuración del monitor de vídeo y cumple con la norma VESA DDC2B.

Capacidad de actualización

Es posible actualizar el firmware de iKVM por medio de la interfaz web del CMC o el comando RACADM `fwupdate`. Para obtener más información, consulte [Administración del iKVM desde el CMC](#).

Interfaces de conexión física

Puede conectarse a un servidor o a la consola CLI del CMC a través del iKVM desde el panel frontal del chasis, una interfaz de consola analógica (ACI) o el panel posterior del chasis.

 **NOTA:** Los puertos del panel de control situado en la parte delantera del chasis están específicamente diseñados para el módulo iKVM, que es opcional. Si no existe un módulo iKVM, no podrán utilizarse estos puertos.

Prioridades de las conexiones del iKVM

Sólo se permite una conexión de iKVM a la vez. El iKVM asigna un orden de prioridad a cada tipo de conexión, de manera que cuando existan varias sólo una esté disponible y las demás queden desactivadas.

El orden de prioridad de las conexiones del iKVM es el siguiente:

1. Panel frontal
2. ACI
3. Panel posterior

Por ejemplo, si existen conexiones en el panel frontal y ACI, la conexión del panel frontal permanecerá activa y la otra quedará desactivada. Si existen conexiones del panel posterior y ACI, las conexiones de ACI tendrán prioridad.

Establecimiento de niveles por medio de la conexión de ACI

El iKVM admite conexiones por niveles con servidores y la consola de línea de comandos del CMC del iKVM, ya sea de forma local a través de un puerto de Remote Console Switch o de manera remota a través del software Dell RCS®. El iKVM admite conexiones de ACI de los siguientes productos:

- 1 Dell Remote Console Switch™ 180AS, 2160AS, 2161DS-2* o 4161DS
- 1 Sistema de conmutación Avocent AutoView®
- 1 Sistema de conmutación Avocent DSR®
- 1 Sistema de conmutación Avocent AMX®

* No admite la conexión de consola de Dell CMC.

 **NOTA:** El iKVM también admite una conexión de ACI con los modelos Dell 180ES y 2160ES, aunque el establecimiento de niveles no es óptimo. Esta conexión requiere un USB para PS2 SIP.

Uso de OSCAR

En esta sección se ofrece una descripción general de la interfaz OSCAR.

Conceptos básicos de navegación

[Tabla 9-1](#) describe las funciones de navegación de la interfaz OSCAR por medio del teclado y el mouse.

Tabla 9-1. Navegación de OSCAR con el teclado y el mouse

Tecla o secuencia de teclas	Resultado
1 <Imprimir pantalla>-<Imprimir pantalla>	Cualquiera de estas secuencias de teclas permiten abrir OSCAR, en función de la configuración para Invocar OSCAR . Puede activar dos, tres o todas las secuencias de teclas seleccionando las casillas Invocar OSCAR del cuadro de diálogo Principal y haciendo clic en Aceptar .
1 <Mayús>-<Mayús>	
1 <Alt>-<Alt>	
1 <Ctrl>-<Ctrl>	
<F1>	Abre la pantalla de Ayuda del cuadro de diálogo actual.
<Esc>	Cierra el cuadro de diálogo actual sin guardar los cambios y regresa al cuadro de diálogo anterior. En el cuadro de diálogo Principal , la tecla <Esc> cierra la interfaz OSCAR y regresa al servidor seleccionado.

	En un cuadro de mensaje, cierra el cuadro emergente y regresa al cuadro de diálogo actual.
<Alt>	Abre cuadros de diálogo, selecciona o marca opciones y ejecuta acciones si se utiliza en combinación con letras subrayadas u otros caracteres designados.
<Alt>+<X>	Cierra el cuadro de diálogo actual y regresa al cuadro de diálogo anterior.
<Alt>+<O>	Selecciona el botón Aceptar y regresa al cuadro de diálogo anterior.
<Intro>	Completa una operación de conmutación en el cuadro de diálogo Principal y sale de OSCAR.
Hacer clic, <Entrar>	En un cuadro de texto, selecciona el texto para editarlo y activa las teclas de flecha izquierda y derecha para desplazar el cursor. Presione <Entrar> nuevamente para salir del modo de edición.
<Imprimir pantalla>, <Retroceso>	Vuelve a la selección anterior si no hubo otras pulsaciones de teclas.
<Imprimir pantalla>, <Alt>+<O>	Desconecta de inmediato a un usuario de un servidor; no se selecciona un servidor. El indicador de estado señala el estado Libre (esta acción sólo se aplica a =<O> en el teclado y no en el teclado numérico).
<Imprimir pantalla>, <Pausa>	Enciende el modo de protector de pantalla de inmediato e impide el acceso a esa consola, si se encuentra protegida con contraseña.
Teclas de flecha hacia arriba/abajo	Desplazan el cursor de línea en línea en las listas.
Teclas de flecha hacia la derecha/la izquierda	Desplazan el cursor entre las columnas al editar un cuadro de texto.
<Inicio>/<Fin>	Desplazan el cursor hacia la parte superior (Inicio) o inferior (Fin) de una lista.
<Suprimir>	Elimina caracteres en un cuadro de texto.
Teclas de número	Se utilizan en el teclado o en el teclado numérico.
<Bloq Mayús>	Desactivada. Para pasar de mayúsculas a minúsculas o viceversa, utilice la tecla <Mayús>.

Configuración de OSCAR

Tabla 9-2 ofrece una descripción de las funciones disponibles en el menú **Configuración** de OSCAR que permiten configurar los servidores.

Tabla 9-2. Funciones del menú de configuración de OSCAR

Componente	Propósito
Menú	Ordena la lista de servidores por número de ranura o alfabéticamente por nombre.
Seguridad	<ul style="list-style-type: none"> 1 Define una contraseña para restringir el acceso a los servidores. 1 Activa un protector de pantalla y define un periodo de inactividad antes de que el protector aparezca y se establezca el modo de protección de pantalla.
Indicador	Cambia la visualización, la duración, el color o la ubicación de los indicadores de estado.
Idioma	Cambia el idioma de todas las pantallas de OSCAR.
Transmisión	Se configura para controlar varios servidores de forma simultánea a través del teclado o el mouse.
Exploración	Define un patrón de exploración personalizado para hasta 16 servidores.

Para acceder al cuadro de diálogo **Configuración**:

1. Pulse <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar**. Aparecerá el cuadro de diálogo **Configurar**.

Cambio de la configuración de la pantalla

Utilice el cuadro de diálogo **Menú** para cambiar el orden en que aparecen los servidores y definir un tiempo de retardo de pantalla para OSCAR.

Para acceder al cuadro de diálogo **Menú**:

1. Presione <Imprimir pantalla> para abrir la interfaz OSCAR. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar** y luego en **Menú**. Aparece el cuadro de diálogo **Menu (Menú)**.

Para elegir el orden predeterminado en que aparecen los servidores en el cuadro de diálogo **Principal**:

1. Seleccione **Nombre** para mostrar los servidores ordenados alfabéticamente por el nombre.
O bien:
Seleccione **Slot (Ranura)** para visualizar los servidores ordenados por número de ranura.

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

Para asignar una o más secuencias de teclas para activar OSCAR:

- Seleccione una secuencia de teclas en el menú **Invocar OSCAR**.
- Haga clic en **OK (Aceptar)**.

La tecla predeterminada para abrir OSCAR es <Imprimir pantalla>.

Para definir un tiempo de retardo de pantalla para OSCAR:

- Ingrese la cantidad de segundos (de 0 a 9) que tardará en abrirse la pantalla de OSCAR después de presionar <Imprimir pantalla>. Si introduce el valor <0> OSCAR se abrirá sin retardo.
- Haga clic en **OK (Aceptar)**.

El tiempo de retardo de la pantalla de OSCAR permite realizar una conmutación no forzada. Para realizar una conmutación no forzada, consulte [Conmutación no forzada](#).

Control de indicadores de estado

El indicador de estado aparece en el escritorio y muestra el nombre del servidor seleccionado o el estado de la ranura seleccionada. Utilice el cuadro de diálogo **Indicador** para configurar el indicador para cada servidor o cambiar el color, la opacidad, la duración y la ubicación del indicador en el escritorio.

Tabla 9-3. **Indicadores de estado de OSCAR**

Indicador	Descripción
	Tipo de indicador por nombre
	Señala que el usuario fue desconectado de todos los sistemas
	Indica que el modo de transmisión se encuentra activado

Para acceder al cuadro de diálogo **Indicador**:

- Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
- Haga clic en **Configurar** y luego en **Indicador**. Aparecerá el cuadro de diálogo **Indicador**.

Para especificar la forma en que aparecerá el indicador de estado:

- Seleccione **En pantalla** para mostrar el indicador todo el tiempo, o bien **En pantalla y por tiempo** para mostrar el indicador sólo durante cinco segundos antes de una conmutación.

 **NOTA:** Si selecciona sólo la opción **Por tiempo**, el indicador no se mostrará.

- Seleccione un color para el indicador en la sección **Color de visualización**. Las opciones son negro, rojo, azul y violeta.
- En **Modo de visualización**, seleccione **Opaco** para que el color del indicador sea sólido o **Transparente** para ver el escritorio a través del indicador.
- Para definir la posición del indicador en el escritorio:
 - Haga clic en **Definir posición**. Aparecerá el cuadro **Definir posición del indicador**.
 - Haga clic con el botón izquierdo del mouse en la barra de título y arrástrela a la posición deseada en el escritorio.
 - Haga clic con el botón derecho del mouse para regresar al cuadro de diálogo **Indicador**.

 **NOTA:** Los cambios realizados en la posición del indicador sólo se guardarán cuando haga clic en **Aceptar** en el cuadro de diálogo **Indicador**.

- Haga clic en **Aceptar** para guardar la configuración.

Para salir sin guardar los cambios, haga clic en .

Administración de servidores con iKVM

El módulo iKVM es una matriz de conmutación analógica que admite hasta 16 servidores. El conmutador iKVM utiliza la interfaz OSCAR para seleccionar y configurar los servidores. Además, incluye una entrada de sistema que permite establecer una conexión de consola de línea de comandos con el CMC.

Compatibilidad con periféricos

El módulo iKVM es compatible con los siguientes periféricos:

- 1 Teclados USB de PC estándar con diseño QWERTY, QWERTZ, AZERTY y japonés 109.
- 1 Monitores VGA con compatibilidad para DDC.
- 1 Dispositivos señaladores USB estándar.
- 1 Concentradores de alimentación propia USB 1.1 conectados al puerto USB local del iKVM.
- 1 Concentradores USB 2.0 conectados a la consola del panel anterior del chasis Dell M1000e.

 **NOTA:** Puede usar varios teclados y mouse en el puerto USB local del iKVM. El módulo acumula las señales de entrada. Si existen señales de entrada simultáneas de varios teclados o mouse USB, los resultados pueden ser impredecibles.

 **NOTA:** Las conexiones USB sirven únicamente para teclados, mouse, concentradores USB admitidos. iKVM no admite datos transmitidos desde otros periféricos USB.

Visualización y selección de servidores

Utilice el cuadro de diálogo **Principal** de OSCAR para ver, configurar y administrar servidores a través de iKVM. Puede ver los servidores por nombre o ranura. El número de ranura corresponde al número de ranura del chasis que ocupa el servidor. La columna **Slot (Ranura)** indica el número de ranura en el que se ha instalado un servidor.

 **NOTA:** La línea de comandos de Dell del CMC ocupa la Ranura 17. Si selecciona esta ranura se mostrará la línea de comandos del CMC, donde podrá ejecutar comandos RACADM remotos o conectarse a servidores y módulos para la depuración de errores.

 **NOTA:** La CMC asigna los nombres de servidor y los números de ranura.

Para acceder al cuadro de diálogo **Main (Principal)**:

Pulse <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Main (Principal)**.

O bien:

Si se ha asignado una contraseña, aparece el cuadro de diálogo **Password (Contraseña)**. Escriba su contraseña y haga clic en **OK (Aceptar)**. Aparece el cuadro de diálogo **Main (Principal)**.

Para obtener más información sobre la configuración de una contraseña, consulte [Configuración de la seguridad de la consola](#).

 **NOTA:** Existen cuatro opciones para invocar la interfaz OSCAR. Puede activar una, varias o todas las secuencias de teclas si selecciona las casillas en la sección **Invocar OSCAR** del cuadro de diálogo **Principal** y hace clic en **Aceptar**.

Cómo ver el estado de los servidores

El estado de los servidores del chasis se indica en las columnas que se encuentran a la derecha del cuadro de diálogo **Principal**. La siguiente tabla describe los símbolos de estado.

Tabla 9-4. Símbolos de estado de la interfaz OSCAR

Símbolos	Descripción
	(Punto verde) El servidor está en línea.
	(X roja) El servidor está fuera de línea o ausente en el chasis.
	(Punto amarillo) El servidor no está disponible.
	(Verde A o B) Acceso al servidor a través del canal de usuario indicado por la letra: A= panel posterior, B= panel frontal.

Selección de servidores

Utilice el cuadro de diálogo **Principal** para seleccionar servidores. Cuando selecciona un servidor, el iKVM reconfigura el teclado y el mouse con los valores apropiados para ese servidor.

- 1 Para seleccionar servidores:

Haga doble clic en el nombre del servidor o el número de ranura.

O bien:

Si los servidores están ordenados por ranura (es decir, si el botón **Ranura** está presionado), escriba el número de ranura y presione <Entrar>.

O bien:

Si los servidores están ordenados por nombre (es decir, si el botón **Nombre** está presionado), escriba los primeros caracteres del nombre del servidor, defínalo como exclusivo y presione <Entrar> dos veces.

- 1 Para seleccionar el servidor anterior:

Presione <Imprimir pantalla> y luego <Retroceso>. Estas teclas permiten alternar entre las conexiones actual y anterior.

- 1 Para desconectar a un usuario de un servidor:

Presione <Imprimir pantalla> para acceder a OSCAR y haga clic en **Desconectar**.

O bien:

Presione <Imprimir pantalla> y luego <Alt><0>. De esta forma el estado será libre, sin servidores seleccionados. Si el indicador de estado está activo, mostrará el estado Libre en el escritorio. Consulte el apartado [Control de indicadores de estado](#).

Conmutación no forzada

Este procedimiento permite alternar los servidores por medio de una secuencia de teclas. Puede realizar una conmutación por software a un servidor pulsando <Impr Pant> y luego escribiendo los primeros caracteres de su nombre o número. Si anteriormente definió un **tiempo de retardo** (la cantidad de segundos que transcurren antes de que el cuadro de diálogo **Principal** aparezca al presionar <Imprimir pantalla>) y presiona la secuencia de teclas antes de que finalice ese plazo, la interfaz OSCAR no se abrirá.

Para configurar OSCAR para la conmutación no forzada:

1. Pulse <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar** y luego en **Menú**. Aparece el cuadro de diálogo **Menu (Menú)**.
3. Seleccione **Nombre** o **Ranura** para la clave de orden/visualización.
4. Escriba el tiempo de retardo deseado expresado en segundos en el campo **Tiempo de retardo de pantalla**.
5. Haga clic en **OK (Aceptar)**.

Para realizar una conmutación no forzada a un servidor:

- 1 Presione <Imprimir pantalla> para seleccionar un servidor.

Si los servidores están ordenados por ranura según la opción elegida en el paso 3 (es decir, si el botón **Ranura** está presionado), escriba el número de ranura y presione <Entrar>.

O bien:

Si los servidores están ordenados por nombre según la opción elegida en el paso 3 (es decir, si el botón **Nombre** está presionado), escriba los primeros caracteres del nombre del servidor para establecerlo como exclusivo y presione <Entrar>.

- 1 Para volver al servidor anterior, presione <Imprimir pantalla> y luego <Retroceso>.

Conexiones de vídeo

El módulo iKVM presenta conexiones de vídeo en los paneles frontal y posterior del chasis. Las señales de conexión del panel frontal tienen prioridad respecto de las del panel posterior. Cuando un monitor se conecta al panel frontal, la conexión de vídeo no se transmite al panel posterior, y aparece un mensaje de OSCAR para indicar que las conexiones del KVM y ACI del panel posterior están desactivadas. Si el monitor se desactiva (es decir, si se retira del panel frontal o se desactiva mediante un comando del CMC), la conexión de ACI se activará y la conexión de KVM permanecerá desactivada. (Para obtener información sobre el orden de prioridad de conexión, consulte [Prioridades de las conexiones del iKVM](#)).

Para obtener información acerca de cómo activar o desactivar la conexión del panel anterior, consulte [Activación o desactivación del panel frontal](#).

Advertencia de apropiación

Habitualmente, un usuario conectado a una consola de servidor a través del iKVM y otro usuario conectado a la misma consola a través de la función de redirección de consola de la interfaz gráfica del usuario de iDRAC tienen el mismo acceso a la consola y pueden escribir de forma simultánea.

Para evitar este escenario, antes de iniciar la redirección de consola de iDRAC, el usuario remoto puede deshabilitar la consola local en la interfaz web del iDRAC. El usuario del iKVM local recibirá un mensaje de OSCAR que indica que otro usuario se apropiará de la conexión en un plazo determinado. El usuario local deberá finalizar su trabajo antes de que se cierre la conexión del iKVM al servidor.

No existe una función de apropiación disponible para el usuario del iKVM.

 **NOTA:** Si un usuario remoto del iDRAC desactivó el video local de un servidor, las funciones de video, teclado y mouse de ese servidor no estarán disponibles para el iKVM. El estado del servidor aparecerá marcado con un punto amarillo en el menú de OSCAR para indicar que se encuentra bloqueado o no disponible para uso local (consulte [Cómo ver el estado de los servidores](#)).

Configuración de la seguridad de la consola

La interfaz OSCAR permite configurar valores de seguridad en la consola del iKVM. Puede establecer un modo de protector de pantalla para que se inicie cuando la consola permanezca inactiva durante un plazo determinado. Cuando se inicia, la consola permanece bloqueada hasta que se presiona una tecla o se mueve el mouse. Para continuar, es necesario ingresar la contraseña del protector de pantalla.

Utilice el cuadro de diálogo **Seguridad** para bloquear la consola mediante protección por contraseña, para definir o cambiar esta contraseña o para activar el protector de pantalla.

 **NOTA:** Si pierde u olvida la contraseña del iKVM, puede restablecer los valores predeterminados de fábrica por medio de la interfaz web del CMC o de RACADM. Consulte el apartado [Eliminación de una contraseña perdida u olvidada](#).

Acceso al cuadro de diálogo Seguridad

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar** y luego en **Seguridad**. Aparecerá el cuadro de diálogo **Seguridad**.

Definición o cambio de contraseña

1. Haga clic una vez y presione <Entrar> o haga doble clic en el campo **Nueva**.
2. Escriba la contraseña nueva en el campo **Nueva** y presione <Entrar>. En las contraseñas se distingue entre mayúsculas y minúsculas y deben tener entre 5 y 12 caracteres. Además deben incluir al menos una letra y un número. Los caracteres válidos son: A-Z, a-z, 0-9, espacio y guión.
3. Escriba nuevamente la contraseña en el campo **Repetir** y presione <Entrar>.
4. Haga clic en **Aceptar** si sólo desea cambiar la contraseña, y luego cierre el cuadro de diálogo.

Protección por contraseña de la consola

1. Defina la contraseña tal como se indica en el procedimiento anterior.
2. Seleccione la casilla **Activar protector de pantalla**.
3. Escriba la cantidad de minutos de **Tiempo de inactividad** (de 1 a 99) para retrasar la protección por contraseña y la activación del protector de pantalla.
4. Para el **Modo**: si el monitor es compatible con ENERGY STAR®, seleccione **Energía**; de lo contrario, seleccione **Pantalla**.

 **NOTA:** Si se define el modo en **Energía**, el monitor entrará en modo inactivo. Para indicar este estado, el monitor se apaga y una luz de color ámbar reemplaza al LED de alimentación de color verde. Si el modo se define en **Pantalla**, la marca OSCAR se desplazará por la pantalla mientras dure la prueba. Antes de comenzar una prueba, aparece un mensaje de advertencia emergente que indica: "El modo de energía puede dañar un monitor no compatible con ENERGY STAR. No obstante, una vez comenzada la prueba es posible cerrarla de inmediato mediante la interacción del teclado o el mouse".

 **PRECAUCIÓN:** Si se utiliza el modo de **Energía** en monitores no compatibles con **Energy Star**, el monitor puede sufrir daños.

5. Opcional: para activar la prueba de protector de pantalla, haga clic en **Prueba**. Aparecerá el cuadro de diálogo **Prueba de protector de pantalla**. Haga clic en **Aceptar** para iniciar la prueba.

La prueba dura 10 segundos. Al finalizar, la pantalla regresará al cuadro de diálogo **Seguridad**.

Conexión

1. Presione <Imprimir pantalla> para abrir la interfaz OSCAR. Aparecerá el cuadro de diálogo **Contraseña**.

2. Escriba la contraseña y haga clic en **Aceptar**. Aparecerá el cuadro de diálogo **Principal**.

Configuración de la desconexión automática

Puede configurar la interfaz OSCAR para que se desconecte automáticamente de un servidor después de un período de inactividad.

1. En el cuadro de diálogo **Principal**, haga clic en **Configurar** y luego en **Seguridad**.
2. En el campo **Tiempo de inactividad**, indique la cantidad de tiempo que desea permanecer conectado a un servidor antes de que se produzca la desconexión automática.
3. Haga clic en **OK (Aceptar)**.

Eliminación de la protección por contraseña de la consola

1. En el cuadro de diálogo **Principal**, haga clic en **Configurar** y luego en **Seguridad**.
2. En el cuadro de diálogo **Seguridad**, haga clic una vez y presione <Entrar> o haga clic dos veces en el campo **Nueva**.
3. Deje en blanco el campo **Nueva** y presione <Entrar>.
4. Haga clic una vez y presione <Entrar> o haga doble clic en el campo **Repetir**.
5. Deje en blanco el campo **Repetir** y presione <Entrar>.
6. Haga clic en **Aceptar** si sólo desea eliminar la contraseña.

Activación del modo de protector de pantalla sin contraseña

 **NOTA:** Si la consola está protegida con contraseña, primero debe eliminar esta función. Siga los pasos del procedimiento anterior antes de proseguir.

1. Seleccione **Activar protector de pantalla**.
2. Escriba la cantidad de minutos (de 1 a 99) que desea retrasar la activación del protector de pantalla.
3. Seleccione **Energía** si el monitor es compatible con ENERGY STAR; de lo contrario, seleccione **Pantalla**.

 **PRECAUCIÓN:** Si se utiliza el modo de Energía en monitores no compatibles con Energy Star, el monitor puede sufrir daños.

4. Opcional: para activar la prueba de protector de pantalla, haga clic en **Prueba**. Aparecerá el cuadro de diálogo **Prueba de protector de pantalla**. Haga clic en **Aceptar** para iniciar la prueba.

La prueba dura 10 segundos. Al finalizar, la pantalla regresará al cuadro de diálogo **Seguridad**.

 **NOTA:** Si se activa el modo de protector de pantalla, el usuario quedará desconectado del servidor, y no se seleccionará ningún servidor. El indicador de estado señalará el estado Libre.

Finalización del modo de protector de pantalla

Para salir del modo de protector de pantalla y regresar al cuadro de diálogo **Principal**, presione cualquier tecla o mueva el mouse.

Para desactivar el protector de pantalla:

1. En el cuadro de diálogo **Seguridad**, deselectione la casilla **Activar protector de pantalla**.
2. Haga clic en **OK (Aceptar)**.

Para activar el protector de pantalla de inmediato, presione <Imprimir pantalla> y luego <Pausa>.

Eliminación de una contraseña perdida u olvidada

Si pierde u olvida la contraseña del iKVM, puede restablecer los valores predeterminados de fábrica y luego cambiar la contraseña. Para restablecer la contraseña utilice la interfaz web del CMC o RACADM.

Para restablecer una contraseña del iKVM perdida u olvidada por medio de la interfaz web del CMC:

1. Inicie sesión en la interfaz web del CMC.
2. En el submenú Chasis, seleccione **iKVM**.
3. Haga clic en la ficha **Configuración**. Se muestra la página **iKVM Configuration (Configuración de iKVM)**.
4. Haga clic en **Restaurar valores predeterminados**.

A continuación puede cambiar la contraseña por medio de OSCAR. Consulte el apartado [Definición o cambio de contraseña](#).

Para restablecer una contraseña perdida u olvidada con RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:

```
racadm racresetcfg -m kvm
```

 **NOTA:** El comando **racresetcfg** restablece los valores para activar el panel anterior y la consola Dell del CMC, si difieren de los valores predeterminados.

Para obtener más información sobre el subcomando **racresetcfg**, consulte [racresetcfg](#).

Cambio de idioma

Utilice el cuadro de diálogo **Idioma** para que el texto de la interfaz OSCAR aparezca en uno de los idiomas admitidos. El texto cambiará inmediatamente al idioma seleccionado en todas las pantallas de la interfaz.

Para cambiar el idioma de OSCAR:

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar** y luego en **Idioma**. Aparecerá el cuadro de diálogo **Idioma**.
3. Haga clic en el botón de radio del idioma deseado, y luego haga clic en **Aceptar**.

Acceso a la información sobre la versión

Utilice el cuadro de diálogo **Versión** para ver las versiones de firmware y hardware del iKVM e identificar la configuración de idioma y teclado.

Para ver la información sobre la versión:

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Comandos** y luego en **Mostrar versiones**. Aparecerá el cuadro de diálogo **Versión**.

En la mitad superior del cuadro de diálogo **Versión** se enumeran las versiones del subsistema del equipo.

3. Haga clic en o presione <Esc> para cerrar el cuadro de diálogo **Versión**.

Exploración del sistema

En el modo de exploración, el iKVM explora automáticamente cada ranura (cada servidor). Es posible explorar hasta 16 servidores especificando los que desea explorar y los segundos que aparecerán en pantalla.

Para agregar servidores a la lista de exploración:

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configurar** y luego en **Explorar**. Aparecerá el cuadro de diálogo **Explorar**, con la lista de todos los servidores en el chasis.
3. Seleccione las casillas de los servidores que desea explorar.

O bien:

Haga doble clic en el nombre del servidor o ranura.

O bien:

Presione <Alt> y el número del servidor que desea explorar. Puede seleccionar hasta 16 servidores.

4. En el campo **Tiempo**, indique la cantidad de segundos (de 3 a 99) que el iKVM debe esperar antes de avanzar al siguiente servidor de la secuencia.
5. Haga clic en el botón **Agregar/Eliminar** y luego en **Aceptar**.

Para eliminar un servidor de la lista **Explorar**:

1. En el cuadro de diálogo **Explorar**, seleccione la casilla correspondiente al servidor que desea quitar.

O bien:

Haga doble clic en el nombre del servidor o ranura.

O bien:

Haga clic en el botón **Borrar** para eliminar todos los servidores de la lista **Explorar**.

2. Haga clic en el botón **Agregar/Eliminar** y luego en **Aceptar**.

Para iniciar el modo de exploración:

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
3. Seleccione la casilla **Activar exploración**.
4. Haga clic en **OK (Aceptar)**. Aparecerá un mensaje para indicar que el mouse y el teclado fueron restablecidos.
5. Haga clic en para cerrar el mensaje.

Para cancelar el modo de exploración:

1. Si la interfaz **OSCAR** está abierta y se muestra el cuadro de diálogo **Principal**, seleccione un servidor de la lista.

O bien:

Si la interfaz **OSCAR** *no* está abierta, mueva el mouse o presione cualquier tecla. La exploración se detendrá en el servidor actualmente seleccionado.

O bien:

Presione <Imprimir pantalla>. Aparecerá el cuadro de diálogo **Principal**. Seleccione un servidor de la lista.

2. Haga clic en el botón **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
3. Deseleccione la casilla **Activar exploración**.

Transmisión a servidores

Puede controlar más de un servidor del sistema a la vez para asegurarse de que todos reciben la misma señal de entrada. Puede optar por transmitir pulsaciones de teclas y movimientos de mouse por separado.

 **NOTA:** Puede transmitir a hasta 16 servidores a la vez.

Para realizar la transmisión a los servidores:

1. Presione <Imprimir pantalla>. Aparece el cuadro de diálogo **Main (Principal)**.
2. Haga clic en **Configuración** y luego en **Transmisión**. Aparecerá el cuadro de diálogo **Transmisión**.

 **NOTA:** Transmisión de pulsaciones de teclas: si utiliza pulsaciones de teclas, el estado del teclado debe ser idéntico para todos los servidores que reciben la transmisión para que la interpretación de las pulsaciones sea la misma. Específicamente, los modos <Bloq Mayús> y <Bloq Num> deben ser iguales en todos los teclados. Mientras el iKVM intenta enviar pulsaciones de teclas a todos los servidores seleccionados a la vez, algunos servidores pueden inhibirse y retrasar la transmisión.

 **NOTA:** Transmisión de movimientos del mouse: para que el mouse actúe correctamente, todos los servidores deben tener los mismos controladores de mouse, pantallas de escritorio (por ejemplo, iconos colocados en lugares idénticos) y resoluciones de vídeo. El mouse también debe estar exactamente en el mismo lugar en todas las pantallas. Dado que es muy difícil cumplir estas condiciones, el uso de movimientos del mouse para la transmisión de señales a varios servidores puede producir resultados impredecibles.

3. Para activar el mouse y/o el teclado para que los servidores recibirán los comandos de transmisión, seleccione las casillas.

O bien:

Presione las flechas hacia arriba o abajo para desplazar el cursor a un servidor de destino. Presione <Alt><K> para seleccionar la casilla del teclado y/o <Alt><M> para seleccionar la del mouse. Repita este procedimiento con los servidores adicionales.

4. Haga clic en **Aceptar** para guardar la configuración y regresar al cuadro de diálogo **Configurar**. Haga clic en o presione <Esc> para regresar al cuadro de diálogo **Principal**.
5. Haga clic en **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
6. Haga clic en la casilla **Activar transmisión** para activarla. Aparecerá el cuadro de diálogo **Advertencia de transmisión**.
7. Haga clic en **Aceptar** para activar la transmisión.

Para cancelarla y regresar al cuadro de diálogo **Comandos**, haga clic en o presione <Esc>.

8. Si la transmisión está activada, escriba la información y/o ejecute los movimientos del mouse que desea transmitir desde la estación de administración. Sólo podrá acceder a los servidores de la lista.

Para desactivar la transmisión:

En el cuadro de diálogo **Comandos**, deseccione la casilla **Activar transmisión**.

Administración del iKVM desde el CMC

Activación o desactivación del panel frontal

Para activar o desactivar el acceso al iKVM desde el panel frontal por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <valor>
```

donde el <valor> es 1 (activar) o 0 (desactivar).

Para obtener más información sobre el subcomando **config**, consulte [config](#).

Para activar o desactivar el acceso al iKVM desde el panel frontal por medio de la interfaz web:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione iKVM en el árbol del sistema. La página muestra **iKVM Status (Estado de iKVM)**.
3. Haga clic en la ficha **Configuración**. Se muestra la página **iKVM Configuration (Configuración de iKVM)**.
4. Para activar, seleccione la casilla **USB/Vídeo de panel anterior activado**.
Para desactivar, deseccione la casilla **USB/Vídeo de panel frontal activado**.
5. Haga clic en **Apply (Aplicar)** para guardar la configuración.

Activación de la consola Dell del CMC a través de iKVM

Para permitir que el iKVM acceda a la consola Dell CMC por medio de RACADM, abra una consola de texto/Telnet en CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

Para activar la consola Dell CMC por medio de la interfaz web:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione iKVM en el árbol del sistema. La página muestra **iKVM Status (Estado de iKVM)**.
3. Haga clic en la ficha **Setup (Configuración)**. Se muestra la página **iKVM Configuration (Configuración de iKVM)**.
4. Seleccione la casilla **Permitir acceso a CLI del CMC desde el iKVM**.
5. Haga clic en **Apply (Aplicar)** para guardar la configuración.

Cómo ver el estado y las propiedades del iKVM

El módulo KVM de acceso local para el chasis del servidor Dell M1000e se denomina módulo de conmutación KVM integrado Avocent®, o iKVM. El estado del iKVM asociado con el chasis puede verse en la página **Estado de las propiedades del chasis** debajo de la sección **Gráficos del chasis**.

Para ver el estado del iKVM a través de **Gráficos de chasis**.

1. Inicie sesión en la interfaz web del CMC.
2. Aparecerá la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado del iKVM. El estado del iKVM se indica mediante el color del gráfico secundario del iKVM:
 - 1 Verde: el iKVM está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el iKVM está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el iKVM está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario del iKVM y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre ese iKVM.
4. El gráfico secundario del iKVM tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del iKVM**.

Para obtener más información acerca de iKVM, consulte [Uso del módulo iKVM](#).

Para ver el estado del iKVM a través de la página **Estado de iKVM**:

1. Inicie sesión en la interfaz web del CMC.
2. En el árbol del sistema, seleccione **iKVM**. Aparecerá la página **Estado del iKVM**.

[Tabla 9-5](#) describe la información proporcionada en la página **Estado de iKVM**.

Tabla 9-5. Información del estado de iKVM

N.º	Descripción
Presencia	Indica si el módulo iKVM está Presente o Ausente .
Estado de la alimentación	Indica el estado de alimentación del iKVM: Encendido , Apagado o N/A (ausente).
Nombre	Muestra el nombre de producto del iKVM.
Fabricante	Muestra el fabricante del iKVM.
Número de parte	Muestra el número de parte del iKVM. El número de parte es un identificador único que el proveedor proporciona.
Versión del firmware	Indica la versión del firmware del iKVM.
Versión del hardware	Indica la versión del hardware del iKVM.
Panel anterior conectado	Indica si el monitor está conectado al conector VGA del panel frontal (Sí o No). Esta información se proporciona al CMC a fin de determinar si el usuario local tiene acceso al panel anterior del chasis.
Panel posterior conectado	Indica si el monitor está conectado al conector VGA del panel posterior (Sí o No). Esta información se proporciona al CMC a fin de determinar si el usuario local tiene acceso al panel posterior del chasis.
Puerto de categorización conectado	El iKVM es completamente compatible con la categorización de conmutadores KVM externos de Dell y Avocent que usan hardware incorporado. Cuando el iKVM se categoriza, se puede tener acceso a los servidores del chasis por medio de la pantalla del conmutador KVM externo desde el cual se categoriza al iKVM.
USB/vídeo del panel anterior activado	Indica si el conector VGA del panel anterior está activado (Sí o No).
Permitir acceso al CMC desde el conmutador iKVM	Indica si la consola de comandos del CMC por medio del iKVM está activada (Sí o No).

Actualización del firmware de iKVM

Es posible actualizar el firmware del iKVM por medio de la interfaz web del CMC o RACADM.

Para actualizar el firmware del iKVM por medio de la interfaz web del CMC:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Actualizar**. Aparecerá la página **Componentes que se pueden actualizar**.
4. Haga clic en el nombre de iKVM. Aparece la página **Firmware Update (Actualización de firmware)**.

5. En el campo **Imagen del firmware**, introduzca la ruta de acceso al archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para desplazarse a la ubicación del archivo.

 **NOTA:** El nombre predeterminado de la imagen del firmware de iKVM es **kvm.bin**; sin embargo, el usuario lo puede cambiar.

6. Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.
7. Haga clic en **Yes (Sí)** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador de estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar en gran medida según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Puntos adicionales para tener en cuenta:
- 1 No utilice el botón **Actualizar** ni visite otra página durante la transferencia del archivo.
 - 1 Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización del archivo**: esta opción sólo está disponible durante la transferencia de archivos.
 - 1 El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

 **NOTA:** La actualización puede llevar hasta un minuto para el iKVM.

Cuando se completa la actualización, iKVM se reinicia y el nuevo firmware se actualiza y aparece en la página **Componentes que se pueden actualizar**.

Para actualizar el firmware del iKVM por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:

```
racadm fwupdate -g -u -a <dirección IP del servidor TFTP> -d <ruta de archivo/nombre de archivo> -m kvm
```

Por ejemplo,

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

Para obtener más información sobre el subcomando **fwupdate**, consulte [fwupdate](#).

Solución de problemas

 **NOTA:** Si tiene una sesión de redirección de consola activa y hay un monitor de menor resolución conectado con el iKVM, la resolución de la consola del servidor puede restablecerse si el servidor se selecciona en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iKVM, Linux cambiará a consola de texto.

Tabla 9-6. Solución de problemas del iKVM

Problema	Probable causa y solución
El mensaje "El usuario fue deshabilitado por el control del CMC" aparece en el monitor conectado al panel frontal.	<p>La conexión del panel frontal fue desactivada por el CMC.</p> <p>Para activar el panel frontal puede utilizar la interfaz web del CMC o RACADM.</p> <p>Para activar el panel frontal por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1. Inicie sesión en la interfaz web del CMC. 2. Seleccione iKVM en el árbol del sistema. 3. Haga clic en la ficha Configuración. 4. Seleccione la casilla USB/Vídeo de panel frontal activado. 5. Haga clic en Apply (Aplicar) para guardar la configuración. <p>Para activar el panel frontal por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1</pre>
No funciona el acceso al panel posterior.	<p>El panel frontal está activado por el CMC, y hay un monitor conectado actualmente al panel.</p> <p>Sólo se permite una conexión a la vez. La conexión del panel frontal tiene prioridad respecto de ACI y el panel posterior. Para obtener más información sobre la prioridad de conexión, consulte Prioridades de las conexiones del iKVM.</p>
El mensaje "El usuario fue deshabilitado porque otro equipo se encuentra actualmente conectado" aparece en el monitor conectado al panel posterior.	<p>Un cable de red está conectado al conector del puerto de ACI del iKVM y a un equipo KVM secundario.</p> <p>Sólo se permite una conexión a la vez. La conexión de ACI tiene prioridad respecto de la del monitor del panel posterior. El orden de prioridad es: panel frontal, ACI y luego el panel posterior.</p>
El indicador LED de color ámbar del iKVM está parpadeando.	<p>Existen tres causas posibles:</p> <p>Existe un problema en el iKVM, por lo que debe reprogramarse. Para solucionar el problema, siga las instrucciones para actualizar el firmware del iKVM (consulte Actualización del firmware de</p>

	<p>iKVM).</p> <p>El módulo iKVM está reprogramando la interfaz de consola del CMC. En este caso, la consola de CMC no se encuentra disponible temporalmente y está representada por un punto de color amarillo en la interfaz OSCAR. Este proceso demora hasta 15 minutos.</p> <p>El firmware del iKVM detectó un error de hardware. Para obtener información adicional, consulte el estado del iKVM.</p> <p>Para ver el estado del iKVM por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1. Inicie sesión en la interfaz web del CMC. 2. Seleccione iKVM en el árbol del sistema. <p>Para ver el estado del iKVM por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:</p> <pre>racadm getkvminfo</pre>
<p>El módulo iKVM está conectado a través del puerto ACI a un conmutador KVM externo, pero ninguna de las entradas de las conexiones de ACI está disponible.</p> <p>Todos los estados muestran un punto amarillo en la interfaz OSCAR.</p>	<p>La conexión del panel frontal está activada y tiene un monitor conectado. Dado que el panel frontal tiene prioridad sobre el resto de las conexiones de iKVM, los conectores ACI y del panel posterior están deshabilitados.</p> <p>Para activar la conexión del puerto ACI, primero debe deshabilitar el acceso al panel frontal o retirar el monitor que tiene conectado. Las entradas de OSCAR del conmutador KVM externo se activarán y estarán disponibles para el acceso.</p> <p>Para desactivar el panel frontal por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1. Inicie sesión en la interfaz web del CMC. 2. Seleccione iKVM en el árbol del sistema. 3. Haga clic en la ficha Configuración. 4. Deseleccione la casilla USB/Vídeo de panel frontal activado. 5. Haga clic en Apply (Aplicar) para guardar la configuración. <p>Para desactivar el panel frontal por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>
<p>En el menú de OSCAR, la conexión de Dell CMC muestra una X de color rojo y no es posible establecer conexión con el CMC.</p>	<p>Existen dos causas posibles:</p> <p>La consola Dell CMC fue desactivada. En este caso, para activarla puede utilizar la interfaz web del CMC o RACADM.</p> <p>Para activar la consola Dell CMC por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1. Inicie sesión en la interfaz web del CMC. 2. En el árbol del sistema, seleccione iKVM. 3. Haga clic en la ficha Configuración. 4. Seleccione la casilla Permitir acceso a CLI del CMC desde el iKVM. 5. Haga clic en Apply (Aplicar) para guardar la configuración. <p>Para activar la conexión de Dell CMC por medio de RACADM, abra una consola de texto SSH/Telnet en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p>El CMC no se encuentra disponible porque se está inicializando, cambiando al CMC en espera o se está reprogramando. En este caso, simplemente aguarde hasta que el CMC finalice el proceso de inicialización.</p>
<p>El nombre de ranura de un servidor muestra el mensaje "Inicializando" en la interfaz OSCAR y no es posible seleccionarlo.</p>	<p>El servidor se está inicializando o el iDRAC de ese servidor sufrió una falla en el proceso de inicialización.</p> <p>Primero espere 60 segundos. Si el servidor aún sigue en el proceso de inicialización, el nombre de ranura aparecerá apenas finalice el proceso y podrá seleccionar el servidor.</p> <p>Si después de 60 segundos la interfaz OSCAR aún indica que la ranura se está inicializando, retire y vuelva a insertar el servidor en el chasis. Esta acción permitirá que el iDRAC se reinicialice.</p>

[Regresar a la página de contenido](#)

Instalación y configuración del CMC

Guía del usuario

- [Antes de comenzar](#)
- [Instalación del hardware del CMC](#)
- [Instalación del software de acceso remoto en una estación de administración](#)
- [Configuración de un explorador de web](#)
- [Configuración del acceso inicial al CMC](#)
- [Acceso al CMC a través de una red](#)
- [Instalación o actualización del firmware de CMC](#)
- [Configuración de las propiedades del CMC](#)
- [Comprensión del entorno de CMC redundante](#)

Esta sección proporciona información acerca de cómo instalar el hardware del CMC, cómo establecer el acceso al CMC y cómo configurar el entorno de administración para utilizar el CMC.

Este capítulo lo guía a través de los siguientes pasos para configurar el CMC:

- 1 Configurar el acceso inicial al CMC
- 1 Acceder al CMC a través de una red
- 1 Agregar y configurar usuarios del CMC
- 1 Actualizar el firmware del CMC

Además, puede encontrar información sobre la instalación y la configuración de entornos de CMC redundantes en [Comprensión del entorno de CMC redundante](#).

Antes de comenzar

Antes de configurar el entorno del CMC, descargue la versión más reciente del firmware del CMC del sitio web de asistencia de Dell en support.dell.com.

Luego, tome el DVD *Dell Systems Management Tools and Documentation* incluido con el sistema:

Instalación del hardware del CMC

Como el CMC ha sido previamente instalado en el chasis, no requiere instalación. Para comenzar con el CMC que está instalado en el sistema, consulte [Instalación del software de acceso remoto en una estación de administración](#).

Usted puede instalar un segundo CMC para que funcione como dispositivo en espera para el CMC principal. Para obtener más información sobre un CMC en espera, consulte [Comprensión del entorno de CMC redundante](#).

Instalación del software de acceso remoto en una estación de administración

Usted puede acceder al CMC por medio de Telnet, Secure Shell (SSH) o las utilidades de consola serie que se incluyen con el sistema operativo o a través de la interfaz web.

Si desea utilizar RACADM remoto desde la estación de administración, deberá instalarla. El sistema incluye el DVD *Dell Systems Management Tools and Documentation*. Este DVD ofrece los siguientes componentes:

- 1 Directorio de raíz del DVD: contiene Dell System Build and Update Utility
- 1 SYSMGMT: contiene productos de software de administración de sistemas incluyendo Dell OpenManage Server Administrator
- 1 Docs: contiene documentación para sistemas, productos de software de administración de sistemas, periféricos y controladores RAID
- 1 SERVICIO: contiene las herramientas que necesita para configurar el sistema, y entrega los últimos diagnósticos y drivers optimizados por Dell para el sistema

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

Instalación de RACADM en una estación de administración con Linux

1. Inicie sesión como root en el sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux Enterprise Server admitido en el que desea instalar los componentes de Managed System.
2. Insert the *Dell Systems Management Tools and Documentation* DVD into the DVD drive.

3. Si es necesario, monte el DVD en una ubicación deseada utilizando el comando `mount` o un comando similar.

 **NOTA:** En el sistema operativo Red Hat Enterprise Linux 5, los DVD se montan automáticamente mediante la opción `-noexec` `mount`. Esta opción no permite iniciar ningún archivo ejecutable desde el DVD. Usted deberá montar manualmente el DVD-ROM y después ejecutar los archivos ejecutables.

4. Desplácese al directorio `SYSMGMT/srvadmin/linux/supportscripts`. Ejecute la secuencia `srvadmin-install.sh` de la siguiente manera:

```
sh srvadmin-install.sh --express
```

O bien:

```
sh srvadmin-install.sh -x
```

La secuencia instala el paquete de software típico para la configuración del sistema.

 **NOTA:** Puede registrar la salida de la instalación de RPM al agregar `2>&1 | tee -a /var/log/srvadmin.log` a la ejecución de la secuencia de shell mencionada anteriormente. El comando resultante es `sh srvadmin-install.sh 2>&1 | tee -a /var/log/srvadmin.log`

5. Inicie los servicios de Server Administrator con el comando de inicio `sh srvadmin-services.sh`.

 **NOTA:** El DVD *Dell Systems Management Tools and Documentation* contiene la versión 5.4 del paquete de software de administración de sistemas Dell OpenManage y la versión 1.0.3 de Dell Systems Build and Update Utility. El directorio raíz del DVD también contiene imágenes ISO de Dell Systems Build and Update Utility (versión 1.0) y del CD *Dell Systems Console and Agent* (software Dell OpenManage versión 5.3.0.1). También puede descargar paquetes web de la versión 5.4 del software de Dell OpenManage Server Administrator y de Dell OpenManage Management Station desde el sitio web de asistencia de Dell, en support.dell.com. Puede transferir el contenido de estos paquetes web a CD o a memorias USB para los sistemas que no tengan unidades de DVD.

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

 **NOTA:** Al utilizar la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo:

```
racadm getconfig -f <nombre de archivo>
```

O bien:

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

Desinstalación de RACADM de una estación de administración con Linux

Abra una consola de texto en la estación de administración y escriba:

```
rpm -e <nombre_del_paquete_de_racadm>
```

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

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

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

Configuración de un explorador de web

Puede configurar y administrar el CMC y los servidores y módulos instalados en el chasis por medio de un explorador de web. Consulte [Exploradores de web compatibles](#) para ver una lista de los exploradores de web que puede utilizar con el CMC.

El CMC y la estación de administración en la que utilice el explorador deben estar en la misma red, que se denomina la *red de administración*. En función de los requisitos de seguridad, la red de administración puede ser una red aislada y muy segura.

Debe asegurarse de que las medidas de seguridad en la red de administración, como los servidores de seguridad y los servidores proxy, no impidan al explorador de web acceder al CMC.

Además, tenga en cuenta que las funciones de algunos exploradores pueden interferir con la conectividad o el rendimiento, en especial si la red de administración no tiene una ruta a Internet. Si la estación de administración está ejecutando un sistema operativo Windows, hay configuraciones de Internet Explorer que pueden interferir con la conectividad, incluso cuando se está utilizando una interfaz de línea de comandos para acceder a la red de administración.

Servidor proxy

Si tiene un servidor proxy para la navegación y éste no tiene acceso a la red de administración, puede agregar las direcciones de la red de administración a la lista de excepciones del explorador. Esto indica al explorador que omita el servidor proxy al momento de acceder a la red de administración.

Internet Explorer

Siga estos pasos para editar la lista de excepciones en Internet Explorer:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Opciones de Internet...**, luego haga clic en **Conexiones**.
3. En la sección **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN...**
4. En la sección **Servidor proxy**, haga clic en **Opciones avanzadas...**
5. En la sección **Excepciones**, agregue a la lista las direcciones de los CMC y los iDRAC en la red de administración, separadas por puntos y comas. Puede utilizar nombres DNS y comodines en sus anotaciones.

Mozilla FireFox

Siga estos pasos para editar la lista de excepción en Mozilla FireFox:

1. Inicie Firefox.
2. Haga clic en **Herramientas**→ **Opciones...**→ **Opciones avanzadas**, luego haga clic en la ficha **Red**.
3. Haga clic en **Configuración...**
4. En el campo **No usar proxy para**, agregue a la lista las direcciones de los CMC y los iDRAC en la red de administración, separadas por comas. Puede utilizar nombres DNS y comodines en sus anotaciones.

Filtro de suplantación de identidad (phishing) de Microsoft®

Si el Filtro de suplantación de identidad (phishing) de Microsoft está activado en Internet Explorer 7 en el sistema de administración y el CMC no tiene acceso a Internet, se pueden experimentar demoras de varios segundos al momento de acceder al CMC, ya sea que esté utilizando el explorador u otra interfaz, como RACADM remoto. Siga estos pasos para desactivar el filtro de suplantación de identidad:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Filtro de suplantación de identidad**, y luego haga clic en **Configuración del filtro de suplantación de identidad**.
3. Marque la casilla **Desactivar el filtro de suplantación de identidad**.
4. Haga clic en **OK (Aceptar)**.

Obtención de la lista de revocación de certificados (CRL)

Si el CMC no tiene una ruta a Internet, usted debe desactivar la función de obtención de la lista de revocación de certificados (CRL) en Internet Explorer. Esta función prueba si un servidor como el servidor de web del CMC está utilizando un certificado que está en una lista de certificados revocados obtenida de la Internet. Si no hay acceso a Internet, esta función puede provocar demoras de varios segundos al momento de acceder al CMC por medio del explorador o con una interfaz de línea de comandos, como RACADM remoto.

Siga estos pasos para desactivar la obtención de CRL:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Opciones de Internet...**, luego haga clic en **Opciones avanzadas**.
3. Desplácese a la sección Seguridad y deseccione **Comprobar si se revocó el certificado del editor**.
4. Haga clic en **OK (Aceptar)**.

Descarga de archivos desde el CMC con Internet Explorer

Cuando utiliza Internet Explorer para descargar archivos desde el CMC puede experimentar problemas cuando la opción **No guardar las páginas cifradas en el disco** está desactivada.

Siga estos pasos para activar la opción **No guardar las páginas cifradas en el disco**:

1. Inicie el Internet Explorer.

2. Haga clic en **Herramientas**→ **Opciones de Internet...**, luego haga clic en **Opciones avanzadas**.
3. Desplácese a la sección Seguridad y marque **No guardar las páginas cifradas en el disco**.

Habilitación de animaciones en Internet Explorer

Al transferir archivos a una interfaz web o desde la misma, un icono de transferencia de archivos gira para mostrar que hay actividad de transferencia. En Internet Explorer, esto requiere que el explorador esté configurado para reproducir animaciones, que es la configuración predeterminada.

Siga estos pasos para configurar Internet Explorer para reproducir animaciones:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Opciones de Internet...**, luego haga clic en **Opciones avanzadas**.
3. Desplácese a la sección Multimedia y marque **Activar animaciones en páginas web**.

Configuración del acceso inicial al CMC

Para administrar el CMC de manera remota, conecte el CMC a la red de administración y luego establezca la configuración de red del CMC. Para obtener información sobre la configuración de los valores de la red del CMC, consulte [Configuración de la red del CMC](#). Esta configuración inicial asigna los parámetros del sistema de red TCP/IP para permitir el acceso al CMC.

El CMC está conectado a la red de administración. Todo el acceso externo al CMC y a los iDRAC se realiza mediante el CMC. Recíprocamente, el acceso a los servidores administrados se realiza mediante conexiones de red a los módulos de E/S (IOM). Esto permite aislar la red de aplicaciones de la red de administración.

Si tiene un chasis, conecte el CMC, y el CMC en espera si está presente, a la red de administración. Si tiene más de un chasis, puede elegir entre la conexión básica, en la que cada CMC está conectado a la red de administración, o una conexión de chasis en cadena margarita, en la que los chasis están conectados en serie y sólo uno está conectado a la red de administración. El tipo de conexión básica utiliza más puertos en la red de administración y proporciona mayor redundancia. El tipo de conexión en cadena margarita utiliza menos puertos en la red de administración pero introduce dependencias entre los CMC, lo que reduce la redundancia del sistema.

Conexión básica del CMC a la red

Para obtener el grado más alto de redundancia, conecte cada CMC a la red de administración. Si el chasis tiene un solo CMC, realice una conexión en la red de administración. Si el chasis tiene un CMC redundante en la ranura del CMC secundario, realice dos conexiones a la red de administración.

Cada CMC tiene dos puertos RJ-45 Ethernet, designados **GB1** (el puerto *de enlace ascendente*) y **STK** (el puerto *de apilamiento*). Con una conexión de cables básica, se conecta el puerto GB1 a la red de administración y se deja el puerto STK sin utilizar.

Conexión en cadena margarita del CMC a la red

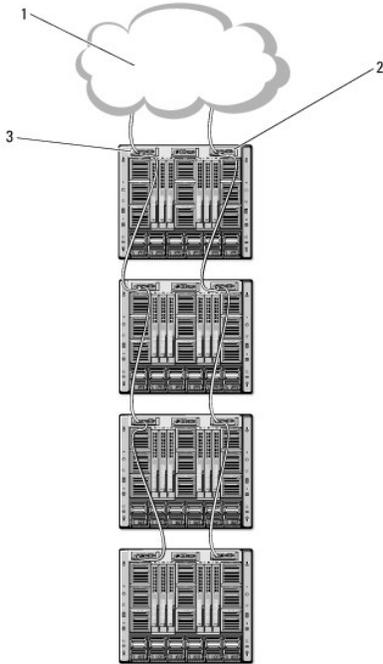
Si tiene varios chasis en un estante, puede reducir el número de conexiones a la red de administración conectando hasta cuatro chasis entre sí en una cadena margarita. Si cada uno de los cuatro chasis tiene un CMC redundante, al conectarlos en una cadena margarita el número de conexiones requeridas de la red de administración se reduce de ocho a dos. Si cada chasis tiene sólo un CMC, las conexiones requeridas se reducen de cuatro a una.

Cuando se conectan varios chasis en cadena margarita entre sí, GB1 es el puerto de enlace ascendente y STK es el puerto de apilamiento. Se debe conectar un puerto GB1 a la red de administración o al puerto STK del CMC en el chasis que esté más cerca de la red. El puerto STK sólo debe recibir una conexión desde un puerto GB1 más lejano en la cadena.

Cree cadenas separadas para los CMC en la ranura principal del CMC y en la segunda ranura del CMC.

[Figura 2-1](#) ilustra la distribución de los cables de cuatro chasis conectados en cadena margarita, cada uno con un CMC en las ranuras principal y secundaria.

Figura 2-1. Conexión en cadena margarita del CMC a la red



1	red de administración	2	CMC secundario
3	CMC principal		

Siga estos pasos para conectar hasta cuatro chasis en cadena margarita:

1. Conecte a la red de administración el puerto GB1 del CMC principal en el primer chasis.
2. Conecte el puerto GB1 del CMC principal en el segundo chasis al puerto STK del CMC principal en el primer chasis.
3. Si tiene un tercer chasis, conecte el puerto GB1 del CMC principal al puerto STK del CMC principal en el segundo chasis.
4. Si tiene un cuarto chasis, conecte el puerto GB1 del CMC principal al puerto STK del tercer chasis.
5. Si tiene CMC redundantes en el chasis, conéctelos utilizando el mismo patrón.

AVISO: El puerto STK en cualquier CMC no se debe conectar nunca a la red de administración. Sólo se puede conectar al puerto GB1 en otro chasis. Conectar un puerto STK a la red de administración puede interrumpir la red y provocar una pérdida de datos.

NOTA: Nunca conecte un CMC principal a un CMC secundario.

NOTA: El restablecimiento de un CMC cuyo puerto STK está conectado en cadena a otro CMC puede interrumpir la red para los CMC que se encuentran más adelante en la cadena. Los CMC subordinados podrían registrar mensajes que indiquen que se ha perdido la conexión con la red y podrían desactivarse y ceder sus funciones a los CMC redundantes.

Configuración de la red del CMC

NOTA: Si cambia la configuración de red del CMC, podría provocar que su conexión de red actual se desconecte.

Puede realizar la configuración inicial de red del CMC antes o después de que el CMC tenga una dirección IP. Si establece la configuración inicial de red del CMC *antes* de tener una dirección IP, puede utilizar cualquiera de las siguientes interfaces:

- 1 El panel LCD en el frente del chasis
- 1 Consola serie del CMC de Dell

Si establece la configuración inicial de red después de que el CMC tenga una dirección IP, puede utilizar cualquiera de las siguientes interfaces:

- 1 Interfaces de línea de comandos (CLI), como una consola serie, Telnet, SSH o la consola CMC de Dell por medio del iKVM
- 1 RACADM remota
- 1 La interfaz web del CMC

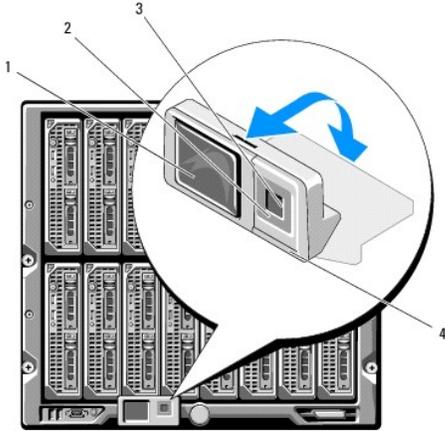
Configuración del sistema de red por medio del asistente de configuración del panel LCD

NOTA: La opción de configurar el CMC mediante el asistente de configuración de LCD sólo estará disponible hasta que se instale el CMC o se cambie la contraseña predeterminada. Si no se cambia la contraseña, se puede continuar usando el LCD para volver a configurar el CMC causando un posible riesgo de seguridad.

El panel LCD se ubica en la esquina inferior izquierda en el frente del chasis.

[Figura 2-2](#) representa el panel LCD.

Figura 2-2. Pantalla LCD



1 Pantalla LCD	2 Botones de desplazamiento (4)
3 Botón de selección ("comprobación")	4 LED indicador de estado

La pantalla LCD muestra menús, iconos, imágenes y mensajes.

El LED indicador de estado en el panel LCD indica la condición general del chasis y de los componentes del mismo.

- 1 Azul continuo indica que está en buenas condiciones.
- 1 Parpadeo en color ámbar indica que al menos un componente tiene una condición de falla.
- 1 Parpadeo en color azul es una señal de identificación que se utiliza para identificar un chasis en un grupo de chasis.

Navegación en la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (hacia arriba, abajo, izquierda y derecha) y un botón central.

- 1 *Para moverse de una pantalla a otra*, utilice los botones de flecha hacia la derecha (siguiente) y hacia la izquierda (anterior). Puede regresar a la pantalla anterior en cualquier momento mientras utiliza el asistente de configuración.
- 1 *Para desplazarse a través de las opciones en una pantalla*, utilice los botones de flecha hacia abajo y hacia arriba.
- 1 *Para seleccionar y guardar un elemento en una pantalla y moverse a la siguiente pantalla*, utilice el botón central.

Para obtener más información acerca de cómo usar el panel LCD, consulte [Uso de la interfaz del panel LCD](#).

Uso del asistente de configuración del panel LCD

1. Si aún no lo ha hecho, oprima el botón de alimentación del chasis para encenderlo.
La pantalla LCD muestra una serie de pantallas de inicialización conforme se enciende. Cuando está listo, muestra la pantalla **Configuración de idioma**.
2. Seleccione el idioma con el botón de flecha hacia abajo, y después oprima el botón central.
Aparecerá la pantalla **Gabinete** con la siguiente pregunta: "¿Desea configurar el gabinete?"
3. Oprima el botón central para avanzar a la pantalla **Configuración de red del CMC**.
4. Seleccione la velocidad de la red (10 Mbps, 100 Mbps, 1 Gbps o Automática) con el botón de flecha hacia abajo.

 **NOTA:** Para obtener el rendimiento efectivo de la red, el valor de la velocidad de la red deberá coincidir con la configuración de la red. Si asigna a la Velocidad de la red un valor menor que la velocidad de la configuración de la red, el consumo de ancho de banda aumentará y la comunicación por medio de la red se hará más lenta. **Determine si la red es compatible con las velocidades de red anteriores y defina el valor según corresponda.** Si la configuración de la red no coincide con ninguno de estos valores Dell recomienda usar la opción Negociación automática (la opción **Automática**) o que consulte al fabricante del equipo de red.

Oprima el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**.

5. Seleccione el modo dúplex (medio o completo) que corresponda al entorno de red.

 **NOTA:** La configuración de la velocidad de la red y de modo dúplex no estará disponible si la negociación automática se establece en Activado o si se selecciona 1000 MB (1 Gbps).

 **NOTA:** Si la negociación automática se activa para un dispositivo pero no para el otro, el dispositivo que utiliza la negociación automática puede determinar la velocidad de la red del otro dispositivo, pero no el modo dúplex; en este caso, el modo dúplex toma el valor predeterminado de dúplex medio durante la negociación automática. Esta incompatibilidad de la configuración de dúplex provocará que la conexión de red sea lenta.

Oprima el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**.

6. Seleccione el modo en el que desea que el CMC obtenga las direcciones IP del NIC:

<p>Protocolo de configuración dinámica de host (DHCP)</p>	<p>El CMC recupera la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente desde un servidor DHCP en la red. El CMC tiene asignada una dirección IP exclusiva en toda la red. Si ha seleccionado la opción DHCP, oprima el botón central. Aparecerá la pantalla ¿Desea registrar el DNS? ; vaya a étape 7.</p>
<p>Estática</p>	<p>Usted introduce manualmente la dirección IP, la puerta de enlace y la máscara de subred en las pantallas que siguen inmediatamente.</p> <p>Si seleccionó la opción Estática, oprima el botón central para avanzar a la siguiente pantalla de Configuración de red del CMC y después:</p> <ol style="list-style-type: none"> a. Establezca la Dirección IP estática utilizando las teclas de flecha hacia la derecha o la izquierda para moverse entre las posiciones, y las teclas de flecha hacia arriba y hacia abajo para seleccionar un número para cada posición. Cuando haya terminado de configurar la Dirección IP estática, oprima el botón central para continuar. b. Establezca la máscara de subred y después oprima el botón central. c. Establezca la puerta de enlace y después oprima el botón central. Aparecerá la pantalla Resumen de la red. <p>La pantalla Resumen de la red muestra los valores de la Dirección IP estática, la Máscara de subred y la Puerta de enlace que usted introdujo. Revise si los valores son correctos. Para corregir un valor, desplácese hacia el botón de flecha hacia la izquierda y luego presione la tecla central para regresar a la pantalla para ese valor. Después de hacer una corrección, oprima el botón central.</p> <ol style="list-style-type: none"> d. Cuando haya confirmado que los valores introducidos son correctos, oprima el botón central. Aparecerá la pantalla ¿Desea registrar el DNS?

7. Si seleccionó Estática en el paso anterior, vaya al paso 8.

Para registrar la dirección IP del servidor DNS, oprima el botón central para continuar. Si no tiene DNS, oprima la tecla de flecha hacia la derecha. Aparecerá la pantalla **¿Desea configurar el iDRAC?** Vaya al paso 8.

Establezca la **Dirección IP de DNS** utilizando las teclas de flecha hacia la derecha o la izquierda para moverse entre las posiciones, y las teclas de flecha hacia arriba y hacia abajo para seleccionar un número para cada posición. Cuando haya terminado de configurar la dirección IP de DNS, oprima el botón central para continuar.

8. Indique si desea configurar el iDRAC:

- o **No:** presione el botón de flecha hacia la derecha. Aparecerá la pantalla **Resumen de IP**. Vaya al paso 9.
- o **Sí:** presione el botón central para continuar.

 **NOTA:** No puede definir una dirección IP estática para la iDRAC mediante el asistente para configuración de LCD. Para establecer una dirección IP estática, use la interfaz web del CMC o RACADM.

Cuando haya hecho su selección, oprima el botón central. Aparecerá la pantalla **Resumen de IP**, mostrando las direcciones IP que usted introdujo.

9. En la pantalla **Resumen de IP**, revise las direcciones IP que proporcionó para asegurar la precisión de las mismas. Para corregir un valor, desplácese hacia el botón de flecha hacia la izquierda y luego presione la tecla central para regresar a la pantalla para ese valor. Después de hacer una corrección, oprima el botón central. De ser necesario, desplácese hacia el botón de flecha hacia la derecha y luego presione la tecla central para regresar a la pantalla **Resumen de IP**.

Una vez que haya confirmado que los valores que ingresó son correctos, presione el botón central. El asistente de configuración se cierra y regresa a la pantalla **Menú principal**.

El CMC está ahora disponible en la red. Puede acceder al CMC en la dirección IP asignada, por medio de la interfaz web o las CLI, por ejemplo, una consola serie, Telnet y SSH.

 **NOTA:** Después de haber completado la configuración de la red a través del asistente de configuración de LCD, el asistente ya no estará disponible.

Acceso al CMC a través de una red

Una vez que haya configurado los valores de red del CMC, puede acceder al CMC remotamente por medio de cualquiera de las siguientes interfaces:

- 1 Interfaz web
- 1 Consola Telnet
- 1 SSH

Telnet está activado a través de una de las otras interfaces; Telnet no es tan seguro como las otras interfaces, por lo tanto, está desactivado de manera predeterminada.

[Tabla 2-1](#) describe cada interfaz de red del CMC.

Tabla 2-1. Interfaces del CMC

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto al CMC por medio de una interfaz gráfica para el usuario. La interfaz web está incorporada en el firmware del CMC y se puede acceder a ella por medio de la interfaz del NIC desde un explorador de web admitido en la estación de administración. Para ver una lista de los exploradores de web admitidos, consulte Exploradores de web compatibles .
Interfaz de línea de comandos de RACADM remoto	Proporciona acceso remoto al CMC desde una estación de administración usando una interfaz de línea de comandos (CLI). RACADM remoto usa la opción <code>racadm -r</code> con la dirección IP del CMC para ejecutar comandos en el CMC.
Telnet	Proporciona acceso de la línea de comandos al CMC a través de la red. La interfaz de línea de comandos RACADM y el comando <code>connect</code> , que se usa para depurar errores del servidor y del módulo de E/S, están disponibles desde la línea de comandos del CMC. NOTA: Telnet es un protocolo no seguro que transmite todos los datos -incluso las contraseñas- en texto simple. Cuando transmita información confidencial, utilice la interfaz SSH.
SSH	Proporciona las mismas capacidades que Telnet mediante una capa de transporte cifrado para tener una mayor seguridad.

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

Puede acceder a las interfaces de web del CMC y del iDRAC a través del NIC del CMC con un explorador de web admitido; también puede iniciarlas desde Dell Server Administrator o Dell OpenManage IT Assistant.

Para ver una lista de los exploradores de web admitidos, consulte [Exploradores de web compatibles](#). Para acceder al CMC a través de un explorador de web admitido, consulte [Acceso a la interfaz web del CMC](#). Para obtener información sobre Dell Server Administrator y Dell OpenManage IT Assistant, consulte [Instalación del software de acceso remoto en una estación de administración](#).

Para acceder a la interfaz del CMC utilizando Dell Server Administrator, ejecute Server Administrator en la estación de administración. En el árbol de sistema que se encuentra en el panel a la izquierda de la página de inicio de Server Administrator, haga clic en Sistema → Chasis del sistema principal → Controlador de acceso remoto. Para obtener más información, consulte la *Guía del usuario de Dell Server Administrator*.

Para acceder a la línea de comandos del CMC a través de Telnet o SSH, consulte [Configuración del CMC para el uso de consolas de línea de comandos](#).

Para obtener más información sobre RACADM, consulte [Uso de la interfaz de línea de comandos de RACADM](#).

Para obtener información sobre la utilización del comando `connect` para conectarse a servidores y módulos de E/S, consulte [Conexión a módulos por medio del comando connect](#).

Instalación o actualización del firmware de CMC

Descarga del firmware de la CMC

Antes de comenzar la actualización del firmware, descargue la versión más reciente del firmware desde el sitio web de asistencia de Dell, en support.dell.com, y guárdela en el sistema local.

En el paquete de firmware de la CMC se incluyen los componentes de software siguientes:

- 1 Datos y código de firmware compilado de la CMC
- 1 Interfaz web, JPEG y otros archivos de datos de la interfaz para el usuario
- 1 Archivos de configuración predeterminados

-  **NOTA:** Durante las actualizaciones del firmware del CMC, algunas o todas las unidades de ventilador en el chasis girarán al 100%. Esto es normal.
-  **NOTA:** De manera predeterminada, la actualización del firmware retendrá la configuración actual del CMC. Durante el proceso de actualización, tiene la posibilidad de restablecer los valores de configuración de la CMC a la configuración predeterminada de fábrica.
-  **NOTA:** Si tiene CMC redundantes instalados en el chasis, es importante actualizar ambos a la misma versión de firmware. Si los CMC tienen versiones de firmware diferentes y se produce una transferencia de funciones ante fallas, podrían ocurrir resultados inesperados.

Puede usar el comando **getsysinfo** de RACADM (consulte [getsysinfo](#)) o la página **Resumen del chasis** (consulte [Cómo ver las versiones actuales del firmware](#)) para ver las versiones actuales de firmware para los CMC instalados en el chasis.

Si tiene un CMC en espera, se recomienda actualizar primero el firmware del CMC en espera. Cuando el CMC en espera se haya actualizado, intercambie las funciones de los CMC, de manera que el CMC recién actualizado se convierta en el CMC principal y el CMC con el firmware más antiguo se convierta en el CMC en espera. (Consulte [cmchangeover](#) para obtener ayuda sobre el intercambio de funciones). Esto permite verificar que la actualización se haya realizado satisfactoriamente y que el nuevo firmware esté funcionando de forma adecuada antes de actualizar el firmware en el segundo CMC. Cuando ambos CMC se hayan actualizado, puede utilizar el comando **cmchangeover** para restaurar los CMC a sus funciones anteriores.

Actualización del firmware del CMC por medio de la interfaz web

Para obtener instrucciones sobre el uso de la interfaz web para actualizar el firmware del CMC, consulte [Actualización del firmware del CMC](#).

Actualización del firmware de la CMC mediante RADCAM

Para obtener instrucciones acerca de cómo utilizar el subcomando **fwupdate** de RACADM para actualizar el firmware del CMC, consulte [fwupdate](#).

Configuración de las propiedades del CMC

Puede configurar las propiedades del CMC, como el presupuesto de alimentación, la configuración de red, los usuarios y las alertas de SNMP y por correo electrónico utilizando la interfaz web o RACADM.

Para obtener más información acerca de cómo usar la interfaz web, consulte [Acceso a la interfaz web del CMC](#). Para obtener más información sobre cómo usar RACADM, consulte [Uso de la interfaz de línea de comandos de RACADM](#).

Puede configurar el CMC usando una de las siguientes herramientas de configuración:

- 1 La interfaz web del CMC. Para obtener más información, consulte [Uso de la interfaz web del CMC](#).
- 1 Una interfaz de línea de comandos (CLI) de RACADM local. Para obtener más información, consulte [Uso de la interfaz de línea de comandos de RACADM](#).

 **AVISO:** Si usa más de una herramienta de configuración del CMC al mismo tiempo, podría obtener resultados inesperados.

Configuración del presupuesto de alimentación

El CMC ofrece un servicio para realizar un presupuesto de alimentación que le permite configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica para el chasis.

El chasis se entrega con tres o seis unidades de suministro de energía (PSU). Si el chasis tiene sólo tres unidades de suministro de energía, usted puede agregar hasta tres más. El servicio de administración de la alimentación permite optimizar el consumo de alimentación y reasignar la alimentación a diferentes módulos según la demanda.

Para obtener más información acerca de la administración de la alimentación en el CMC, consulte [Administración de la alimentación](#).

Para obtener instrucciones acerca de cómo configurar el presupuesto de alimentación y otros valores de la alimentación usando la interfaz web, consulte [Configuración del presupuesto de alimentación](#).

Cómo establecer la configuración de red del CMC

 **NOTA:** Si cambia la configuración de red del CMC, podría provocar que su conexión de red actual se desconecte.

Puede configurar los valores de red del CMC usando una de las siguientes herramientas:

- 1 RACADM: consulte [Configuración de múltiples CMC en varios chasis](#)

 **NOTA:** Si va a instalar el CMC en un entorno de Linux, consulte [Instalación de RACADM en una estación de administración con Linux](#).

- 1 Interfaz web: consulte [Configuración de las propiedades de red del CMC](#)

Cómo agregar y configurar usuarios

Puede agregar y configurar usuarios del CMC usando la RACADM o la interfaz web del CMC. También puede utilizar Microsoft® Active Directory® para

administrar usuarios.

Para obtener instrucciones sobre cómo agregar o configurar usuarios a través de RACADM, consulte [Cómo agregar un usuario del CMC](#). Para obtener instrucciones sobre cómo agregar o configurar usuarios a través de la interfaz web, consulte [Cómo agregar y configurar usuarios del CMC](#).

Para obtener instrucciones sobre cómo usar Active Directory con el CMC, consulte [Uso del CMC con Microsoft Active Directory](#).

Agregar alertas de SNMP y por correo electrónico

Usted puede configurar el CMC para generar alertas de SNMP y/o por correo electrónico cuando ocurren ciertos sucesos del chasis. Para obtener más información, consulte las secciones [Cómo configurar alertas SNMP](#) y [Configuración de alertas por correo electrónico](#).

Comprensión del entorno de CMC redundante

Puede instalar un CMC en espera que tome el control si el CMC principal falla.

Las transferencias de funciones ante fallas puede ocurrir cuando usted:

- 1 Ejecute el comando **cmchangeover** de RACADM. Consulte el apartado [cmchangeover](#).
- 1 Ejecuta el comando **racreset** de RACADM en el CMC activo. Consulte el apartado [racreset](#).
- 1 Desconecta el cable de red del CMC activo
- 1 Desmonta el CMC activo del chasis
- 1 Inicia un flash del firmware del CMC en el CMC activo
- 1 El CMC principal ya no es funcional

 **NOTA:** En caso de una transferencia de funciones ante fallas del CMC, se perderán todas las conexiones de iDRAC y todas las sesiones activas del CMC. Los usuarios que hayan perdido su sesión se deberán volver a conectar al nuevo CMC principal.

Acerca del CMC en espera

El CMC en espera es idéntico y se mantiene como un duplicado del CMC activo. Los CMC activo y en espera se deben instalar con la misma revisión del firmware. Si las revisiones del firmware son diferentes, el sistema informará que hay redundancia degradada.

El CMC en espera asume la misma configuración y propiedades del CMC principal. Debe mantener la misma versión del firmware en ambos CMC, pero no es necesario duplicar los valores de configuración en el CMC en espera.

 **NOTA:** Para obtener información acerca de la instalación de un CMC en espera, consulte el *Manual del propietario del hardware*. Para obtener instrucciones sobre la instalación del firmware de CMC en el CMC en espera, siga las instrucciones en [Instalación o actualización del firmware de CMC](#).

Proceso de elección del CMC principal

No hay ninguna diferencia entre las dos ranuras del CMC; es decir, la ranura no indica la jerarquía. En vez de ello, el CMC que se instala o se inicia primero asume la función del CMC activo. Si se aplica corriente alterna con dos CMC instalados, el CMC instalado en la ranura 1 del chasis del CMC (la izquierda) generalmente se convierte en el CMC activo. El CMC activo se indica con el LED azul.

Si se insertan dos CMC en un chasis que ya está encendido, la negociación automática de activo/en espera puede tomar hasta dos minutos. El funcionamiento normal del chasis se reanuda cuando la negociación se completa.

Planificación de la instalación de CMC redundantes

Al hacer planes para la instalación del CMC y la conexión de cables del chasis, se recomienda elegir el CMC izquierdo para que actúe como el CMC principal y el CMC derecho para que actúe como el secundario, y conservar esas funciones. Esto se recomienda porque es el arreglo predeterminado cuando el chasis se enciende y la redundancia aumenta cuando todos los CMC principales en un chasis conectado en cadena margarita están conectados entre sí. Cuando se produce una transferencia de funciones ante fallas y un CMC en la ranura derecha se convierte en el principal, use el comando **cmchangeover** de RACADM para restablecer el CMC de la ranura izquierda como el principal.

Obtención de la condición del CMC redundante

Puede ver la condición del CMC en espera en la interfaz web. Para obtener más información sobre el acceso al estado del CMC en la interfaz web, consulte [Cómo ver los gráficos del chasis y el estado de los componentes](#).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Administración de la estructura de red de E/S

Guía del usuario

- [Administración de la estructura de red](#)
- [Configuraciones no válidas](#)
- [Ejemplo de encendido por primera vez](#)
- [Supervisión de la condición del módulo de E/S](#)

El chasis puede tener hasta seis módulos de E/S (IOM), que pueden ser módulos de paso o de conmutación.

Los módulos de E/S se clasifican en tres grupos: A, B y C. Cada grupo tiene dos ranuras: la ranura 1 y la ranura 2. Las ranuras se designan con letras, de izquierda a derecha, a lo largo de la parte posterior del chasis: A1 | B1 | C1 | C2 | B2 | A2. Cada servidor tiene ranuras para dos tarjetas intermedias (MC) para conectar a los módulos de E/S. La MC y el módulo de E/S correspondiente deben tener la misma estructura de red.

El chasis admite tres tipos de estructura de red o de protocolo. Los módulos de E/S en un grupo deben tener tipos de estructura de red iguales o compatibles.

- 1 El **grupo A** está siempre conectado a los adaptadores Ethernet integrados del servidor; por lo tanto, el tipo de estructura de red del grupo A siempre será Ethernet.
- 1 En el **grupo B**, las ranuras de los módulos de E/S están conectadas permanentemente a la ranura de la **primera MC (tarjeta intermedia)** en cada módulo del servidor.
- 1 En el **grupo C**, las ranuras de los módulos de E/S están conectadas permanentemente a la **segunda MC (tarjeta intermedia)** en cada módulo del servidor.

Además, cada MC puede admitir dos vínculos externos. Por ejemplo, en la primera MC, el primer vínculo está conectado permanentemente a la ranura 1 del grupo B, y el segundo vínculo está conectado permanentemente a la ranura 2 del grupo B.

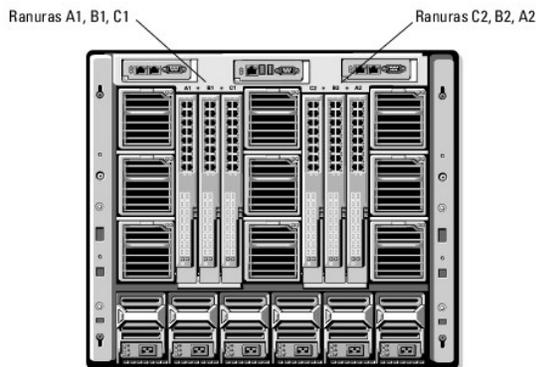
 **NOTA:** En la CLI del CMC, se hace referencia a los módulos de E/S mediante la convención conmutador-*n*: A1=conmutador-1, A2=conmutador-2, B1=conmutador-3, B2=conmutador-4, C1=conmutador-5 y C2=conmutador-6.

Administración de la estructura de red

La administración de la estructura de red le ayuda a evitar y a corregir cualquier problema relacionado con el sistema eléctrico, la configuración o la conectividad ocasionados por la instalación de un módulo de E/S que tiene una estructura de red distinta de la del servidor o sus tarjetas intermedias. Las configuraciones de hardware no válidas podrían ocasionar problemas eléctricos o funcionales en el chasis o sus componentes. Sin embargo, no todas las configuraciones válidas son necesariamente configuraciones admitidas. La administración de la estructura de red sólo evita las que las configuraciones no válidas se activen.

[Figura 10-1](#) muestra la ubicación de los módulos de E/S en el chasis. La ubicación de cada módulo de E/S en el chasis se indica mediante su número de grupo (A, B o C) y número de ranura (1 ó 2). En el chasis, los nombres de las ranuras de los módulos de E/S están marcados como A1, A2, B1, B2, C1 o C2.

Figura 10-1. Vista posterior de un chasis, que muestra la ubicación de los módulos de E/S



El CMC crea anotaciones en el registro de hardware y en los registros del CMC ante configuraciones de hardware no válidas.

Por ejemplo,

- 1 Una MC (tarjeta intermedia) Ethernet conectada a un módulo de E/S de Fibre Channel es una configuración no válida. Sin embargo, una MC Ethernet conectada a un conmutador de Ethernet y a un módulo de E/S de paso de Ethernet instalada en el mismo grupo de módulos de E/S es una conexión válida.
- 1 Un módulo de E/S de paso de Fibre Channel y un módulo de E/S de conmutación de Fibre Channel en las ranuras B1 y B2 es una configuración válida si las primeras tarjetas intermedias en todos los servidores también son de Fibre Channel. En esta caso, el CMC encenderá los módulos de E/S y los servidores. Sin embargo, es posible que cierto software de redundancia de Fibre Channel no admita esta configuración.

 **NOTA:** La verificación de la estructura de red para las tarjetas intermedias de los servidores se realiza sólo cuando el chasis se enciende. Cuando el chasis está con alimentación en espera, los iDRAC en los módulos del servidor permanecen apagados y por lo tanto no pueden informar el tipo de estructura de red de las tarjetas intermedias del servidor. Es posible que el tipo de estructura de red de las tarjetas intermedias no se informe en la interfaz para el usuario del CMC hasta que se encienda el iDRAC en el servidor.

Configuraciones no válidas

Hay tres tipos de configuraciones no válidas:

- 1 Configuración de MC (tarjeta intermedia) no válida, en la que la estructura de red de una tarjeta intermedia recién instalada es diferente a la estructura de red del módulo de E/S existente
- 1 Configuración de módulo de E/S y tarjeta intermedia no válida, en la que la estructura de red del módulo de E/S y de la tarjeta intermedia recién instalados no coinciden o son incompatibles
- 1 Configuración de módulo de E/S y módulo de E/S no válida, en la que un módulo de E/S recién instalado tiene un tipo de estructura de red diferente o incompatible con un módulo de E/S ya instalado en este grupo

Configuración no válida de tarjeta intermedia (MC)

Una configuración no válida de MC se produce cuando la tarjeta intermedia de un solo servidor no es compatible con el módulo de E/S correspondiente. En este caso, todos los demás servidores en el chasis pueden estar funcionando.

Configuración no válida de tarjeta intermedia del módulo de E/S

El módulo de E/S incompatible se mantendrá en estado apagado. El CMC agrega una anotación a los registros del CMC y de hardware que indica la configuración no válida y especifica el nombre del módulo de E/S. El CMC también hará que el LED de error del módulo fallido de E/S parpadee. Si el CMC está configurado para enviar alertas, envía alertas por correo electrónico y/o alertas SNMP para este suceso.

Para obtener información sobre los registros del CMC y de hardware, consulte [Cómo ver los registros de sucesos](#).

Configuración no válida entre módulos de E/S

El CMC mantiene un módulo de E/S recién instalado en estado apagado, hace que el LED de error del módulo de E/S parpadee y crea anotaciones en los registros del CMC y de hardware acerca de la incompatibilidad.

Para obtener información sobre los registros del CMC y de hardware, consulte [Cómo ver los registros de sucesos](#).

Ejemplo de encendido por primera vez

Cuando el chasis se conecta y se enciende, los módulos de E/S tienen prioridad sobre los servidores. Se permite al primer módulo de E/S en cada grupo encenderse antes que los demás. En este momento no se realiza ninguna verificación de los tipos de estructura de red. Si no hay ningún módulo de E/S en la primera ranura de un grupo, se enciende el módulo que está en la segunda ranura de ese grupo. Si ambas ranuras tienen módulos de E/S, se compara el módulo en la segunda ranura el módulo que está en la primera para ver si son congruentes.

Después de que los módulos de E/S se encienden, los servidores se encienden y el CMC verifica la congruencia de la estructura de red de los servidores.

Se permite un módulo de paso y uno de conmutación en el mismo grupo, siempre y cuando sus estructuras de red sean idénticas. Los módulos de conmutación y de paso pueden existir en el mismo grupo, incluso si fueron fabricados por proveedores distintos.

Supervisión de la condición del módulo de E/S

La condición de los módulos de E/S puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de los módulos de E/S**. La página **Gráficos del chasis** proporciona una descripción gráfica de los módulos de E/S instalados en el chasis.

Para ver la condición de los módulos de E/S a través de Gráficos del chasis:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene la condición de los módulos de E/S. La condición de los módulos de E/S se indica por el color del gráfico secundario de los módulos de E/S:
 - 1 Verde: el módulo de E/S está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el módulo de E/S está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el módulo de E/S está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario individual del módulo de E/S y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre dicho módulo de E/S.
4. El gráfico secundario del módulo de E/S tiene un hipervínculo a la página correspondiente de GUI del CMC para proporcionar una exploración inmediata a la página de **Estado de los módulos de E/S** relacionada con dicho módulo de E/S.

Para ver la condición de todos los módulos de E/S a través de la página **Estado de los módulos de E/S**:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **I/O Modulos (Módulos de E/S)** en el menú Chassis (Chasis) del árbol del sistema.
3. Haga clic en la ficha **Propiedades**.
4. Haga clic en la subficha **Estado**. Aparecerá la página **Estado de los módulos de E/S**.

[Tabla 10-1](#) ofrece descripciones de la información que se proporciona en la página **Estado de los módulos de E/S**.

Tabla 10-1. Información de la condición de los módulos de E/S

N.º	Descripción
Presente	Indica si el módulo de E/S está Presente o Ausente .
Estado	 En buen estado Indica que el módulo de E/S está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar la condición del módulo de E/S.
	 Informativo Muestra información acerca del módulo de E/S cuando no se ha producido ningún cambio en la condición (En buen estado, Advertencia, Grave).
	 Advertencia Indica que sólo se han generado alertas de advertencia y que se debe realizar una acción correctiva dentro del tiempo establecido por el administrador . Si no se realizan acciones correctivas dentro del tiempo especificado por el administrador, se pueden producir fallas críticas o graves que pueden afectar la integridad del módulo de E/S. Ejemplos de condiciones que causan advertencias: incompatibilidad de la estructura de red del módulo de E/S con la estructura de red de la tarjeta intermedia del servidor; configuración del módulo de E/S no válida, en la que los módulos de E/S recién instalados no corresponden con el módulo de E/S existente en el mismo grupo.
	 Grave Indica que se ha emitido al menos una alerta de falla. El estado Grave representa una falla del sistema en el módulo de E/S y se debe realizar una acción correctiva inmediatamente . Ejemplos de condiciones que causan un estado Grave: Se detectó una falla en el módulo de E/S; módulo de E/S eliminado.
<p>NOTA: Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener más información, consulte Cómo ver los registros de sucesos.</p>	
Ranura	Indica la ubicación del módulo de E/S en el chasis mediante el número de grupo (A, B, o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1, C2 .
Estructura de red	Indica el tipo de estructura de red para el módulo de E/S: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, Derivación PCIe de 1ª generación, Derivación PCIe de 2ª generación. NOTA: Para evitar incompatibilidades de módulos de E/S en el mismo grupo, es crucial conocer los tipos de estructura de red de los módulos de E/S en el chasis. Para obtener información sobre la estructura de red de E/S, consulte Administración de la estructura de red de E/S .
Nombre	Muestra el nombre del producto del módulo de E/S.
Estado de alimentación	Indica el estado de la alimentación del módulo de E/S: Encendido, Apagado o N/A (Ausente).
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo que Dell asigna para fines de asistencia técnica y mantenimiento. Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener más información, consulte Cómo ver los registros de sucesos . NOTA: Los módulos de paso no tienen etiquetas de servicio. Sólo los módulos de conmutación tienen etiquetas de servicio.

Cómo ver la condición de un módulo de E/S individual

La página **Estado del módulo de E/S** (separada de la página *Estado de los módulos de E/S*) proporciona una descripción general de un módulo de E/S individual

Para ver la condición de un módulo de E/S individual:

1. Inicie sesión en la interfaz web del CMC.
2. Expanda **Módulos de E/S** en el árbol del sistema. Todos los módulos de E/S (1-6) aparecen en la lista **Módulos de E/S** expandida.

3. Haga clic en el módulo de E/S que desea ver en la lista **Módulos de E/S** en el árbol del sistema.

4. Haga clic en la subficha **Estado**. Aparecerá la página **Estado de los módulos de E/S**.

[Tabla 10-2](#) ofrece descripciones de la información que se proporciona en la página **Estado del módulo de E/S**.

Tabla 10-2. Información de la condición del módulo de E/S

N.º	Descripción	
Nombre	Muestra el nombre del módulo de E/S.	
Presente	Indica si el módulo de E/S está Presente o Ausente .	
Estado	 En buen estado	Indica que el módulo de E/S está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar la condición del módulo de E/S.
	 Informativo	Muestra información acerca del módulo de E/S cuando no se ha producido ningún cambio en la condición (En buen estado, Advertencia, Grave). Ejemplos de condiciones que causan un estado informativo: Se detectó la presencia del módulo de E/S; un usuario solicitó un ciclo de encendido del módulo de E/S.
	 Advertencia	Indica que sólo se han generado alertas de advertencia y que se debe realizar una acción correctiva dentro del tiempo establecido por el administrador . Si no se realizan acciones correctivas dentro del tiempo especificado por el administrador, se pueden producir fallas críticas o graves que pueden afectar la integridad del módulo de E/S. Ejemplos de condiciones que causan advertencias: incompatibilidad de la estructura de red del módulo de E/S con la estructura de red de la tarjeta intermedia del servidor; configuración del módulo de E/S no válida, en la que los módulos de E/S recién instalados no corresponden con el módulo de E/S existente en el mismo grupo.
	 Grave	Indica que se ha emitido al menos una alerta de falla. El estado Grave representa una falla del sistema en el módulo de E/S y se debe realizar una acción correctiva inmediatamente . Ejemplos de condiciones que causan un estado Grave: Se detectó una falla en el módulo de E/S; módulo de E/S eliminado.
<p>NOTA: Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener información acerca de cómo ver los registros, consulte Cómo ver el registro de hardware y Cómo ver el registro del CMC.</p>		
Ubicación	Indica la ubicación del módulo de E/S en el chasis mediante el número de grupo (A, B, o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2 .	
Estado de alimentación	Indica el estado de la alimentación del módulo de E/S: Encendido, Apagado o N/A (Ausente).	
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo que Dell asigna para fines de asistencia técnica y mantenimiento.	
Estructura de red	Indica el tipo de estructura de red para el módulo de E/S: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, Derivación PCIe de 1ª generación, Derivación PCIe de 2ª generación. NOTA: Para evitar incompatibilidades de módulos de E/S en el mismo grupo, es crucial conocer los tipos de estructura de red de los módulos de E/S en el chasis. Para obtener información sobre la estructura de red de E/S, consulte Administración de la estructura de red de E/S .	
MAC Address	Muestra la dirección MAC para el módulo de E/S. La dirección MAC es una dirección exclusiva que el proveedor del hardware asigna al dispositivo como una forma de identificación. NOTA: Los módulos de paso no tienen direcciones MAC. Sólo los módulos de conmutación tienen direcciones MAC.	
Función	Muestra los miembros apilables del módulo de E/S cuando los módulos se vinculan entre sí: <ul style="list-style-type: none"> ○ Miembro: el módulo es parte de un conjunto de pilas. ○ Principal: el módulo es un punto de acceso primario. 	

Configuración de valores de red para un módulo de E/S individual

La página Configuración de los módulos de E/S le permite configurar los valores de red del servidor para configurar y administrar el módulo de E/S en el chasis. Para los conmutadores de Ethernet, lo que está configurado es el puerto de administración fuera de banda (dirección IP). El puerto de administración en banda (es decir, VLAN1) no se configura por medio de la interfaz.

-  **NOTA:** Para cambiar los valores de la página Configuración de los módulos de E/S, debe tener privilegios de Administrador de estructura de red A para configurar los módulos de E/S del grupo A; privilegios de Administrador de estructura de red B para configurar los módulos de E/S del grupo B, o privilegios de Administrador de estructura de red C para configurar los módulos de E/S del grupo C.
-  **NOTA:** Para los conmutadores de Ethernet, las direcciones IP de administración en banda (VLAN1) y fuera de banda no pueden ser las mismas o estar en la misma red; esto provocará que no se configure la dirección IP fuera de banda. Consulte la documentación sobre el módulo de E/S para la dirección IP de administración en banda predeterminada.
-  **NOTA:** Sólo se muestran los módulos de E/S presentes en el chasis.
-  **NOTA:** No intente configurar los valores de red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Para configurar los valores de red para un módulo de E/S individual:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Módulos de E/S** en el árbol del sistema. Haga clic en la subficha **Configuración**. Aparecerá la página **Configuración de los valores de red de los módulos de E/S**.
3. Para configurar los valores de red para los módulos de E/S, escriba/seleccione valores para las siguientes propiedades, y luego haga clic en **Aplicar**.

 **NOTA:** Sólo se pueden configurar los módulos de E/S que estén encendidos.

 **NOTA:** La dirección IP establecida en los módulos de E/S a partir del CMC no se guarda en la configuración inicial permanente del conmutador. Para guardar la configuración de la dirección IP de forma permanente, debe introducir el comando connect switch-n de RACADM o usar una interfaz directa a GUI del módulo de E/S para guardar esta dirección en el archivo de configuración inicial.

N.º	Descripción
Ranura	Indica la ubicación del módulo de E/S en el chasis mediante el número de grupo (A, B, o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2. (El valor de las ranuras no se puede cambiar).
Nombre	Muestra el nombre del producto del módulo de E/S. (El nombre del módulo de E/S no se puede cambiar).
Estado de la alimentación	Muestra el estado de la alimentación del módulo de E/S. (El estado de la alimentación no se puede cambiar desde esta página).
DHCP activado	Habilita al módulo de E/S del chasis a solicitar y obtener automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP). Valor predeterminado: seleccionado (activado). Si esta opción está seleccionada, el módulo de E/S recupera automáticamente la configuración de IP (dirección IP, máscara de subred y puerta de enlace) de un servidor DHCP en la red. NOTA: Cuando esta función está activada, los campos de propiedades Dirección IP, Puerta de enlace y Máscara de subred (ubicados inmediatamente después de esta opción) están desactivados, y cualquier valor ingresado previamente para estas propiedades se ignorará. Si esta opción no está seleccionada, debe introducir manualmente una dirección IP, una puerta de enlace y una máscara de subred válida en los campos de texto correspondientes que siguen a esta opción.
Dirección IP	Especifica la dirección IP para la interfaz de red del módulo de E/S.
Máscara de subred	Especifica la máscara de subred para la interfaz de red del módulo de E/S.
Puerta de enlace	Especifica la puerta de enlace para la interfaz de red del módulo de E/S.

Solución de problemas de los valores de red del módulo de E/S

La siguiente lista contiene elementos para solucionar problemas de los valores de red del módulo de E/S:

- 1 El CMC puede leer la configuración de la dirección IP muy rápido después de un cambio de configuración; mostrará 0.0.0.0 después de hacer clic en **Aplicar**. Debe hacer clic en el botón actualizar para ver si la dirección IP está configurada correctamente en el conmutador.
- 1 Si se comete un error al configurar la IP/máscara/puerta de enlace, el conmutador no establecerá la dirección IP y mostrará 0.0.0.0 en todos los campos. Errores comunes:
 - 1 Configurar la dirección IP fuera de banda igual a, o en la misma red que, la dirección IP de administración en banda.
 - 1 Introducir una máscara de subred no válida.
 - 1 Configurar la puerta de enlace predeterminada a una dirección que no está en una red directamente conectada al conmutador.

Para obtener más información sobre los valores de red del módulo E/S, consulte el documento *Información importante de Dell™ PowerConnect™ M6220 Switch y el Artículo de Dell™ PowerConnect™ 6220 Series Port Aggregator*.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Descripción general del CMC

Guía del usuario

- [Funciones de administración del CMC](#)
- [Funciones de seguridad](#)
- [Descripción general del chasis](#)
- [Especificaciones del hardware](#)
- [Conexiones de acceso remoto admitidas](#)
- [Plataformas admitidas](#)
- [Exploradores de web compatibles](#)
- [Aplicaciones admitidas de la consola de administración](#)
- [Compatibilidad con WS-Management](#)
- [Otros documentos útiles](#)

El Dell™ Chassis Management Controller (CMC) es una solución de hardware y software de acoplamiento activo para la administración de sistemas diseñada para proporcionar capacidades de administración remota y funciones de control de la alimentación para los sistemas de chasis Dell M1000e.

Usted puede configurar el CMC para enviar alertas por correo electrónico o de capturas de SNMP para advertencias o errores relacionados con temperaturas, configuraciones erróneas de hardware, interrupciones de la alimentación y velocidades de los ventiladores.

El CMC, que tiene su propio microprocesador y memoria, recibe alimentación del chasis modular en el que está conectado.

Para comenzar con el CMC, consulte [Instalación y configuración del CMC](#).

Funciones de administración del CMC

El CMC proporciona las siguientes funciones de administración:

- 1 Entorno redundante del CMC
 - 1 Registro de Sistema de nombres de dominio dinámico (DNS)
 - 1 Administración y supervisión remotas del sistema por medio de SNMP, una interfaz web, iKVM o una conexión de Telnet o SSH
 - 1 Compatibilidad con la autenticación de Microsoft® Active Directory®: centraliza las identificaciones de usuarios y las contraseñas del CMC en Active Directory por medio del esquema estándar o el esquema extendido
 - 1 Supervisión: brinda acceso a la información del sistema y al estado de los componentes
 - 1 Acceso a registros de sucesos del sistema: proporciona acceso al registro de hardware y al registro del CMC
 - 1 Actualizaciones de firmware para varios componentes: CMC, servidores, iKVM y dispositivos de infraestructura de los módulos de E/S
 - 1 Integración del software de Dell OpenManage™: permite iniciar la interfaz web del CMC desde Dell OpenManage Server Administrator o IT Assistant
 - 1 Alerta del CMC: alerta sobre problemas potenciales del nodo administrado por medio de un mensaje por correo electrónico o una captura SNMP
 - 1 Administración remota de la alimentación: proporciona funciones remotas de administración de la alimentación, como el apagado y el restablecimiento de cualquier componente del chasis, desde una consola de administración
 - 1 Informe de uso de la alimentación
 - 1 Cifrado de Capa de conexión segura (SSL): ofrece administración remota y segura de sistemas por medio de la interfaz web
 - 1 Administración de seguridad de nivel de contraseña: evita el acceso no autorizado a un sistema remoto
 - 1 Autoridad en base a funciones: proporciona permisos asignables para distintas tareas de administración de sistemas
 - 1 Punto de inicio para la interfaz web de Integrated Dell Remote Access Controller (iDRAC)
 - 1 Compatibilidad con WS-Management (para obtener más información, consulte [Compatibilidad con WS-Management](#))
 - 1 Función FlexAddress: reemplaza las identificaciones World Wide Name/Media Access Control (WWN/MAC) asignadas de fábrica con identificaciones WWN/MAC asignadas por el chasis para una ranura particular; una actualización opcional (para obtener más información, consulte [Uso de FlexAddress](#))
 - 1 Gráfico de la condición y del estado del componente del chasis
 - 1 Asistencia para servidores simples o con ranuras múltiples
-

Funciones de seguridad

El CMC proporciona las siguientes funciones de seguridad:

- 1 Autenticación de usuarios por medio de Active Directory (opcional) o identificaciones y contraseñas de usuarios almacenadas en hardware
- 1 Autoridad en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- 1 Configuración de identificaciones y contraseñas de usuarios por medio de la interfaz web
- 1 La interfaz web admite cifrado SSL 3.0 de 128 bits y cifrado SSL 3.0 de 40 bits (para países en los que no se admiten 128 bits)

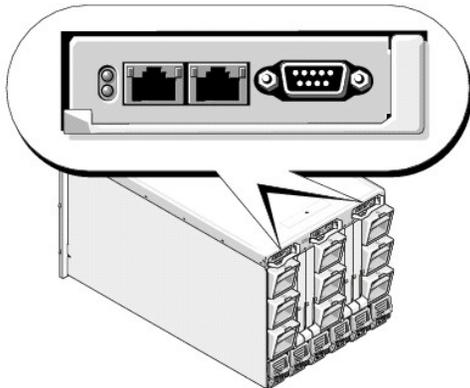
 **NOTA:** Telnet no admite el cifrado SSL.

- 1 Puertos IP que se pueden configurar (en los casos correspondientes)
- 1 Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando ésta ha superado el límite
- 1 Tiempo de interrupción de sesión automático configurable y cantidad de sesiones simultáneas
- 1 Rango limitado de direcciones IP para clientes que se conectan al CMC
- 1 Secure Shell (SSH), que utiliza una capa cifrada para ofrecer una mayor seguridad

Descripción general del chasis

[Figura 1-1](#) muestra el borde delantero de un CMC (inserto) y las ubicaciones de las ranuras del CMC en el chasis.

Figura 1-1. Chasis y CMC Dell M1000e



Especificaciones del hardware

Puertos TCP/IP

Debe proporcionar la información del puerto al abrir servidores de seguridad para tener acceso remoto a un CMC.

[Tabla 1-1](#) identifica los puertos en los que el CMC detecta si hay conexiones de servidor. [Tabla 1-2](#) identifica los puertos que el CMC utiliza como clientes.

Tabla 1-1. Puertos de detección de servidores del CMC

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP
161	Agente SNMP
443*	HTTPS
* Puerto configurable	

Tabla 1-2. Puerto cliente del CMC

Número de puerto	Función
25	SMTP
53	DNS
68	Dirección IP asignada por DHCP

69	TFTP
162	captura SNMP
636	LDAPS
3269	LDAPS para catálogo global (GC)

Conexiones de acceso remoto admitidas

La [tabla 1-3](#) muestra una lista de las funciones de conexión.

Tabla 1-3. Conexiones de acceso remoto admitidas

Conexión	Características
NIC del CMC	<ul style="list-style-type: none"> 1 Ethernet de 10 Mbps/100 Mbps/1 Gbps mediante el puerto GbE del CMC 1 Compatibilidad con DHCP 1 Capturas SNMP y notificación de sucesos por correo electrónico 1 Interfaz de red dedicada para la interfaz web del CMC 1 Interfaz de red para el iDRAC y los módulos de E/S (IOM) 1 Compatibilidad con la consola de comandos Telnet/SSH y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema
Puerto serie	<ul style="list-style-type: none"> 1 Compatibilidad con la consola serie y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema 1 Compatibilidad con intercambio binario para aplicaciones diseñadas específicamente para comunicarse mediante un protocolo binario con un tipo particular de módulo de E/S 1 El puerto serie se puede cambiar para los módulos de E/S por medio del comando connect
Otras conexiones	<ul style="list-style-type: none"> 1 Acceso a la consola del CMC de Dell por medio del módulo de conmutación KVM integrado Avocent® (iKVM)

Plataformas admitidas

El CMC admite sistemas modulares diseñados para la plataforma M1000e. Para obtener información acerca de la compatibilidad con el CMC, consulte la documentación para su dispositivo.

Para ver las plataformas admitidas más recientes, consulte la *Guía de compatibilidad de Dell PowerEdge* ubicada en el sitio web de asistencia de Dell, en support.dell.com.

Exploradores de web compatibles

[Tabla 1-4](#) muestra los exploradores de web admitidos como clientes del CMC.

Para obtener la información más reciente acerca de los exploradores de web admitidos, consulte la *Guía de compatibilidad de Dell OpenManage Server Administrator* ubicada en el sitio web de asistencia de Dell, en support.dell.com.

Tabla 1-4. Exploradores de web compatibles

Sistema operativo	Explorador de web admitido
Windows®	Internet Explorer® 6.0 (de 32 bits) con Service Pack 2 (SP2) para Windows XP y Windows 2003 R2 SP2 solamente. Internet Explorer 7.0 para Windows Vista®, Windows XP y Windows 2003 R2 SP2 solamente.
Linux	Mozilla Firefox 1.5 (de 32 bits) para SUSE® Enterprise Linux (versión 10) solamente. Mozilla Firefox 2.0 (de 32 bits).

Para ver las versiones localizadas de la interfaz web del CMC:

1. Abra el **Panel de control** de Windows.
2. Haga doble clic en el icono **Opciones regionales**.
3. Seleccione la opción regional deseada en el menú desplegable **Su idioma (ubicación)**.

Aplicaciones admitidas de la consola de administración

El CMC admite la integración con Dell OpenManage IT Assistant. Para obtener más información, consulte la documentación de OpenManage IT Assistant.

Compatibilidad con WS-Management

El firmware del CMC incluye una implementación de la especificación WS-Management. WS-Management, una nueva especificación de servicios de web sobre un protocolo basado en SOAP para la administración de sistemas, proporciona un idioma universal para que los dispositivos puedan compartir datos, de forma que se puedan administrar más fácilmente.

El acceso a WS-Management requiere privilegios de usuario de administrador (o root) utilizando la autenticación básica sobre un protocolo de capa de conexión segura (SSL) en el puerto 443. Para obtener información acerca de la configuración de cuentas de usuario, consulte [cfgSessionManagement](#).

Los datos disponibles mediante WS-Management son un subconjunto de datos proporcionados por la interfaz de instrumentación del CMC asignada a los siguientes perfiles de DMTF versión 1.0.0:

- 1 Perfil de capacidades de asignación
- 1 Perfil métrico básico
- 1 Perfil básico del servidor
- 1 Perfil de sistema computacional
- 1 Perfil de sistema modular
- 1 Perfil de propiedad física
- 1 Perfil de asignación de alimentación de Dell
- 1 Perfil de suministro de energía de Dell
- 1 Perfil de topología de la alimentación de Dell
- 1 Perfil de administración del estado de la alimentación
- 1 Perfil de registro de perfiles
- 1 Perfil de registro
- 1 Perfil de asignación de recursos
- 1 Perfil de autorización basada en funciones
- 1 Perfil de sensores
- 1 Perfil de procesador de servicio
- 1 Perfil de administración de identidad simple

Para obtener más información, consulte www.dmtf.org/standards/profiles/. Para ver las actualizaciones para esta lista o información, consulte las notas de publicación de WS-Management o al archivo léame.

La implementación de WS-Management cumple con la especificación de servicios de web DMTF para administración (WS-Management) versión 1.0.0. Las herramientas compatibles conocidas que admiten el protocolo WS-Management incluyen (entre otras) las herramientas de CLI de OpenWSMan y Microsoft WinRM.

Para obtener asistencia específica para WS-Management, consulte la documentación de la aplicación de administración. Hay documentación adicional disponible en la web:

- 1 www.wbemsolutions.com/ws_management.html
- 1 Especificaciones DMTF para WS-Management: www.dmtf.org/standards/wbem/wsman
- 1 Perfiles de administración de DMTF: www.dmtf.org/standards/profiles/

Otros documentos útiles

Además de esta *Guía del usuario*, los siguientes documentos proporcionan información adicional sobre la configuración y el funcionamiento del CMC. Es posible acceder a todos estos documentos en <http://support.dell.com>:

- 1 La ayuda en línea para el CMC proporciona información sobre el uso de la interfaz web.
- 1 Las *Especificaciones técnicas de Chassis Management Controller (CMC) Secure Digital (SD) Card* proporcionan información mínima sobre el uso, la instalación y la versión del BIOS y el firmware.
- 1 La *Guía del usuario de Integrated Dell Remote Access Controller con firmware versión 1.0* proporciona información acerca de la instalación, la configuración y el mantenimiento del iDRAC en sistemas administrados y de administración.
- 1 La *Guía del usuario de Dell OpenManage™ IT Assistant* ofrece información sobre IT Assistant.
- 1 Documentación específica para la aplicación de consola de administración de otros fabricantes.
- 1 La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- 1 La *Guía del usuario de Dell Update Packages* proporciona información acerca de cómo obtener y usar los Dell Update Packages como parte de su

estrategia de actualización del sistema.

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

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

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

- 1 Es posible que se incluyan notas de la versión o archivos Léame para proporcionar actualizaciones de última hora relativas al sistema o a la documentación, o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- 1 Para obtener más información sobre las configuraciones de red de los módulos de E/S, consulte el documento *Información importante de Dell™ PowerConnect™ M6220 Switch* y el *artículo Dell™ PowerConnect™ 6220 Series Port Aggregator*.

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Administración de la alimentación

Guía del usuario

- [Información general](#)
- [Políticas de redundancia](#)
- [Configuración y administración de energía](#)

Información general

El chasis M1000e se entrega con tres o unidades de suministro de energía (PSU) o seis, que es el máximo. Si el chasis tiene tres unidades de suministro de energía, usted puede agregar hasta tres más.

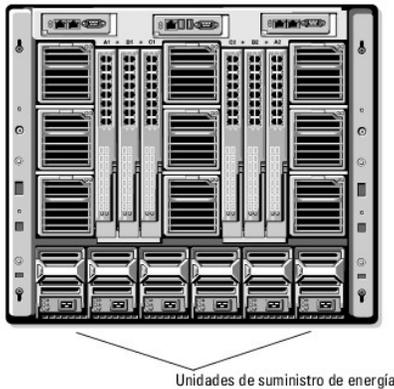
Las unidades de suministro de energía proporcionan energía al chasis y a todos los módulos en el mismo: CMC, IOM, iKVM, ventiladores, LCD del panel anterior y servidores. El CMC administra el presupuesto de alimentación para todos los módulos del chasis.

Para que la redundancia de CA funcione en una configuración de seis unidades de suministro de energía, las tres unidades de suministro de energía a la izquierda se deben conectar a una red de corriente alterna, mientras que las tres a la derecha se conectan a otra. La redundancia de CA no está disponible en una configuración de tres unidades de suministro de energía. Cada unidad de suministro de energía ayuda al CMC a administrar la distribución de la alimentación a los módulos.

Presupuesto de alimentación para módulos de hardware

El CMC asigna alimentación a algunos de los módulos en el chasis M1000e dinámicamente cuando se instalan en el chasis.

Figura 8-1. Chasis con configuración de seis unidades de suministro de energía



Acoplamiento dinámico de unidades de suministro de energía

El acoplamiento dinámico de unidades de suministro de energía es una opción configurable que permite al CMC conservar energía apagando las unidades de suministro de energía no utilizadas y manteniéndolas en modo de espera en caso de que se requiera más alimentación. Esto ahorra energía al aumentar la utilización de las unidades de suministro de energía que permanecen activas, de forma que se utilizan más eficazmente.

Los factores que causan que una unidad de suministro de energía individual o un conjunto de ellas cambie a modo de espera incluyen:

- 1 Población de módulos
- 1 El número de unidades de suministro de energía en el chasis
- 1 La política de redundancia
- 1 Las capacidades y el punto de eficacia máxima de la configuración de la unidad de suministro de energía

Para mantener la eficacia óptima, el CMC utiliza esta información para determinar cuántas unidades de suministro de energía se requieren para alimentar una configuración dada y colocar a las unidades de suministro de energía excedentes en espera. Si se instalan módulos nuevos, el CMC podría activar nuevos suministros, dependiendo de las necesidades y la optimización.

Políticas de redundancia

La política de redundancia es un conjunto configurable de propiedades que determina la forma en que el CMC administra la alimentación al chasis. Las siguientes políticas de redundancia son configurables con acoplamiento dinámico de unidad de suministro de energía o sin acoplamiento:

- 1 Redundancia de CA
- 1 Redundancia del suministro de energía
- 1 Sin redundancia

Usted puede seleccionar y configurar una política de redundancia o utilizar la política de redundancia predeterminada para el chasis. La configuración de la redundancia predeterminada para el chasis depende de cuántas unidades de suministro de energía haya configuradas para el mismo, como se muestra en [tabla 8-1](#).

Tabla 8-1. Configuración de redundancia predeterminada

Configuración de la unidad de suministro de energía	Política de redundancia predeterminada	Configuración predeterminada del acoplamiento dinámico de unidades de suministro de energía
Seis unidades de suministro de energía	Redundancia de CA	Desactivado
Tres unidades de suministro de energía	Sin redundancia	Desactivado

Redundancia de CA

Para que el modo de redundancia de CA funcione con la alimentación óptima, debe tener seis unidades de suministro de energía en el chasis. Puede establecer el chasis para que funcione en el modo de redundancia de CA con menos de seis unidades de suministro de energía, pero no funcionará en un estado degradado.

En el modo de redundancia de CA, las seis unidades de suministro de energía estarán activas. Las tres unidades de suministro de energía a la izquierda deben estar conectadas a una red de CA, mientras que las tres unidades de suministro de energía a la derecha debe estar conectadas a otra red de CA.

- ➡ **AVISO:** Para evitar una falla del sistema y para que la redundancia de CA funcione eficazmente, debe asegurarse de que cada conjunto de unidades de suministro de energía esté conectado a una red de CA separada.

En caso de que una red de CA falle, las tres unidades de suministro de energía en la red de CA en funcionamiento toman el control sin interrumpir a los servidores o a la infraestructura.

- ➡ **AVISO:** En el modo de redundancia de CA, una diferencia en el número de unidades de suministro de energía entre las dos redes de CA (por ejemplo, tres unidades de suministro de energía en una red de CA y dos en la otra) provocará una degradación de la redundancia.

Redundancia del suministro de energía

La capacidad de una unidad de suministro de energía en el chasis se mantiene como repuesto, asegurando que una falla de cualquiera de las unidades de suministro de energía no ocasione que los servidores o el chasis se apaguen. El modo redundancia del suministro de energía requiere cuatro unidades de suministro de energía que funcionen correctamente; cualquier unidad de suministro de energía adicional no se utilizará. La falla de dos unidades de suministro de energía podría ocasionar que se apaguen los servidores en el chasis.

Sin redundancia

Se utiliza la alimentación de hasta tres unidades de suministro de energía para alimentar el chasis completo.

- ➡ **AVISO:** El modo sin redundancia utiliza sólo tres unidades de suministro de energía sin unidades de respaldo. La falla de una de las tres unidades de suministro de energía que se están utilizando podría ocasionar que los servidores pierdan energía y datos.

Conservación de la energía y cambios en el presupuesto de alimentación

El CMC puede llevar a cabo la conservación de la energía cuando se llega al límite de alimentación máxima configurado por el usuario. Cuando la demanda de alimentación excede el límite de energía que se ha establecido, el CMC reduce la alimentación a los servidores a los que se ha asignado una prioridad menor para liberar energía para los servidores con prioridad mayor y a otros módulos en el chasis.

Si todas o varias ranuras en el chasis están configuradas con el mismo nivel de prioridad, el CMC disminuye la alimentación a los servidores según el orden de los números de ranura. Por ejemplo, si los servidores en las ranuras 1 y 2 tienen el mismo nivel de prioridad, la alimentación para el servidor en la ranura 1 se reduce antes que la del servidor en la ranura 2.

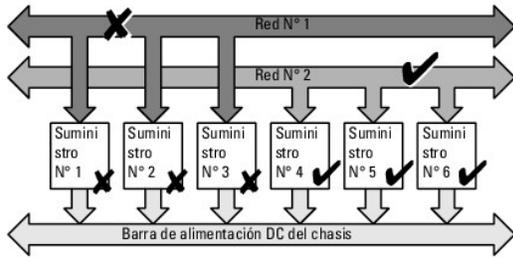
- 📌 **NOTA:** Puede asignar un nivel de prioridad a cada uno de los servidores en el chasis asignándole un número de servidor del 1 al 9 inclusive. El nivel de prioridad predeterminado para todos los servidores es 1. Cuanto menor es el número, mayor es el nivel de prioridad. Para obtener instrucciones acerca de cómo asignar niveles de prioridad a los servidores, consulte [Uso de RACADM](#).

Falla de una unidad de suministro de energía con una política sin redundancia

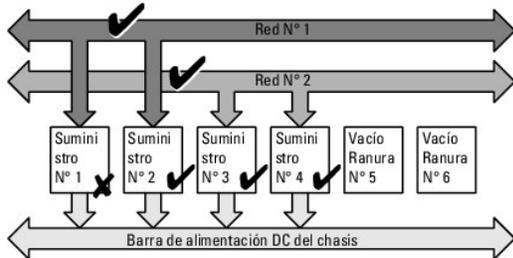
El CMC reduce la alimentación a los servidores cuando se produce un suceso de alimentación insuficiente, como la falla de una unidad de suministro de energía. Después de reducir la alimentación a los servidores, el CMC vuelve a evaluar las necesidades de alimentación del chasis. La alimentación para los servidores con mayor prioridad se restaura en incrementos mientras las necesidades de alimentación permanecen dentro del presupuesto de alimentación.

- 📌 **NOTA:** Para establecer la política de redundancia, consulte [Configuración de redundancia de alimentación y consumo máximo](#).

Figura 8-2. Redundancia de CA (parte superior) y redundancia del suministro de energía (parte inferior)

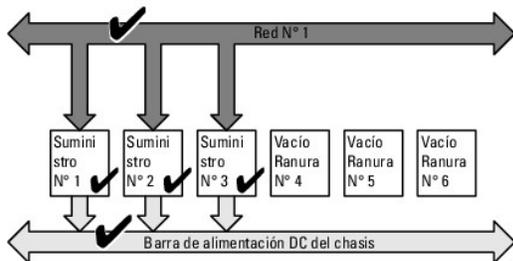


Red doble:
Protege contra fallas de una red de CA



Red doble o simple:
La redundancia del suministro de energía protege contra fallas de un suministro de energía único.

Figura 8-3. Sin redundancia



Red simple:
No proporciona protección contra fallas de red de alimentación o del suministro de energía.

Política de acoplamiento de servidores nuevos

Cuando se enciende un servidor nuevo, podría ser necesario que el CMC reduzca la alimentación a los servidores con menor prioridad para permitir más energía para el servidor nuevo si la adición del nuevo servidor excede la alimentación disponible para el sistema. Esto podría suceder si el administrador ha configurado un límite de alimentación para que es menor que lo que se requeriría para la asignación de toda la energía para los servidores, o si no hay alimentación suficiente para la necesidad de energía de todos los servidores del chasis en el peor de los casos. Si no se puede liberar suficiente energía al reducir la energía asignada de los servidores con menor prioridad, es posible que el nuevo servidor no se pueda iniciar.

La alimentación más alta sostenida requerida para hacer funcionar el chasis y todos los servidores con alimentación máxima, incluyendo el nuevo, es el requisito de alimentación en el peor de los casos. Si esa alimentación está disponible, entonces no se asigna a ningún servidor energía menor a la necesitada en el peor de los casos y se puede encender el nuevo servidor.

Si el requisito de alimentación en el peor de los casos no está disponible, la alimentación se reduce para los servidores con menor prioridad hasta que se libera suficiente alimentación para iniciar el nuevo servidor.

- 1 Si no se puede liberar suficiente energía mediante la reducción de la alimentación para los servidores existentes, es posible que el nuevo servidor no se pueda iniciar.
- 1 Si se libera suficiente energía mediante la reducción de la alimentación para los servidores existentes, la energía liberada se asigna al nuevo servidor y se permite que éste se inicie.

Tabla 8-2 describe las acciones realizadas por el CMC cuando se enciende un nuevo servidor en las condiciones descritas arriba.

Tabla 8-2. Respuesta del CMC cuando se intenta encender un servidor

--	--

La alimentación en el peor de los casos está disponible	Respuesta del CMC	Encendido del servidor
Sí	No se requiere la conservación de energía	Permitido
No	Se realiza la conservación de energía:	
	1 La alimentación requerida para el nuevo servidor está disponible	Permitido
	1 La alimentación requerida para el nuevo servidor no está disponible	No permitido

Tabla 8-3 describe la respuesta del firmware al apagado o el desmontaje de una unidad de suministro de energía conforme se aplica a diversas configuraciones de redundancia de las unidades de suministro de energía.

Tabla 8-3. Impacto en el chasis de la falla o el desmontaje de una unidad de suministro de energía

Configuración de la unidad de suministro de energía	Unidad de suministro de energía dinámica Acoplamiento	Respuesta del firmware
Redundancia de CA	Desactivado	Se alerta al usuario sobre la pérdida de la redundancia de CA.
Redundancia del suministro de energía	Desactivado	Se alerta al usuario de la pérdida de la redundancia del suministro de energía.
Sin redundancia	Desactivado	Se disminuye la alimentación a los servidores con menor prioridad.
Redundancia de CA	Activado	Se alerta al usuario sobre la pérdida de la redundancia de CA. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar el presupuesto de alimentación perdido debido a la falla o desmontaje de una unidad de suministro de energía.
Redundancia del suministro de energía	Activado	Se alerta al usuario de la pérdida de la redundancia del suministro de energía. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar el presupuesto de alimentación perdido debido a la falla o desmontaje de una unidad de suministro de energía.
Sin redundancia	Activado	Se disminuye la alimentación a los servidores con menor prioridad.

Desmontaje de una unidad de suministro de energía con una política sin redundancia

Es posible que el CMC comience a conservar energía cuando un usuario desmonta una unidad de suministro de energía o una cuerda de la CA de una unidad de suministro de energía. El CMC reduce la alimentación para los servidores con menor prioridad hasta que el consumo de energía sea admitido por las unidades de suministro de energía restantes en el chasis. Si se apaga o se desmonta más de una unidad de suministro de energía, el CMC vuelve a evaluar las necesidades de alimentación cuando se desmonta la segunda unidad de suministro de energía para determinar la respuesta del firmware.

Límites

- 1 El CMC no admite el apagado *automatizado* de un servidor con menor prioridad para permitir el encendido de un servidor con mayor prioridad; sin embargo, usted puede realizar apagados iniciados por el usuario.
- 1 Los cambios a la política de redundancia de las unidades de suministro de energía están limitados por el número de unidad de suministro de energía en el chasis. El chasis M1000e se entrega con una de dos configuraciones: tres unidades de suministro de energía o seis unidades de suministro de energía. Usted puede seleccionar cualquiera de los tres valores de configuración de la redundancia de las unidades de suministro de energía enumeradas en [Políticas de redundancia](#). Sin embargo, algunas políticas de redundancia, como la redundancia de CA, no están disponibles para chasis con menos de seis unidades de suministro de energía (el número máximo permitido por chasis).

Configuración y administración de energía

Usted puede utilizar las interfaces web y RACADM para administrar y configurar los controles de alimentación en el CMC. Expresamente, usted puede:

- 1 Ver las asignaciones, el consumo y el estado de la alimentación del chasis, los servidores y las unidades de suministro de energía
- 1 Configurar el presupuesto de alimentación y la redundancia para el chasis
- 1 Ejecutar operaciones de control de alimentación (encendido, apagado, restablecimiento del sistema, ciclo de encendido) en el chasis

Cómo ver la condición de las unidades de suministro de energía

La página **Condición del suministro de energía** muestra el estado y las lecturas de las unidades de suministro de energía asociadas con el chasis. Para obtener más información acerca de la administración de la alimentación en el CMC, consulte [Administración de la alimentación](#).

Por medio de la interfaz web

El estado de las unidades de suministro de energía puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado del suministro de energía**. La página **Gráficos del chasis** proporciona una descripción gráfica de todas las unidades de suministro de energía instaladas en el chasis.

Para ver el estado de todas las unidades de suministro de energía a través de **Gráficos del chasis**:

1. Inicie sesión en la interfaz web del CMC.
2. Aparecerá la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de todas las unidades de suministro de energía. El estado de la unidad de suministro de energía se indica mediante el color del gráfico secundario de la unidad de suministro de energía:
 - 1 Verde: la unidad de suministro de energía está presente, encendida y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: la unidad de suministro de energía está presente, pero es posible que esté encendida o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: la unidad de suministro de energía está presente y apagada. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario de una unidad de suministro de energía individual y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre esa unidad de suministro de energía.
4. El gráfico secundario de la unidad de suministro de energía tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del suministro de energía** para todas las unidades de suministro de energía.

Para ver el estado de las unidades de suministro de energía a través de **Estado del suministro de energía**:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Suministros de energía** en el árbol del sistema. Aparecerá la página **Estado del suministro de energía**.

[Tabla 8-4](#) ofrece descripciones de la información que se proporciona en la página **Estado del suministro de energía**.

Tabla 8-4. Información de la condición del suministro de energía

N.º	Descripción	
Presente	Indica si la unidad de suministro de energía está Presente o Ausente .	
Estado	 En buen estado	Indica que la unidad de suministro de energía está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y la unidad de ventilador, el CMC no puede obtener ni mostrar la condición de la unidad de suministro de energía.
	 Advertencia	Indica que sólo se han emitido alertas de advertencia y que se debe realizar una acción correctiva dentro del marco de tiempo establecido por el administrador. Si no se realizan acciones correctivas dentro del tiempo especificado por el administrador, se podrían producir fallas críticas o graves que pueden afectar la integridad del chasis.
	 Grave	Indica que se ha emitido al menos una alerta de falla. El estado de falla indica una falla de alimentación en el chasis y se debe realizar una acción correctiva inmediatamente .
Nombre	Muestra el nombre de la unidad de suministro de energía: PS- <i>n</i> , donde <i>n</i> es el número del suministro de energía.	
Estado de alimentación	Indica el estado de la alimentación de los suministros de energía (uno de los siguientes): Inicializando , En línea , En espera , En diagnóstico , Fallido , Redundante , Desconectado o Ausente (perdido).	
Capacidad	Muestra la capacidad de alimentación en vatios.	

Uso de RACADM

Consulte [Cómo ver el estado del presupuesto de alimentación](#) a continuación.

Cómo ver el estado del presupuesto de alimentación

El CMC proporciona descripciones generales del estado de la alimentación del subsistema de energía en la página **Estado del presupuesto de alimentación**.

Por medio de la interfaz web

 **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione Chassis (Chasis) en el árbol del sistema.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Se muestra la página **Power Budget Status (Estado de consumo máximo)**.

Tabla 8-5 a la [tabla 8-11](#) describen la información que se muestra en la página **Estado del presupuesto de alimentación**.

Consulte [Configuración de redundancia de alimentación y consumo máximo](#) para obtener información acerca de cómo configurar los valores para esta información.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getpbinfo
```

 **NOTA:** Para obtener más información acerca de `getpbinfo`, incluso los detalles de mensajes de salida, consulte [getpbinfo](#).

Tabla 8-5. Estadísticas de alimentación de tiempo real

N.º	Descripción
Alimentación de entrada en el sistema	Indica el consumo acumulado actual de energía de todos los módulos en el chasis medido desde la entrada de las unidades de suministro de energía. El valor para la alimentación de entrada del sistema se indica en vatios y en BTU/h.
Consumo máximo de alimentación del sistema	Muestra el nivel máximo de consumo de alimentación de entrada en el sistema desde la última vez que se borró el valor. Esta propiedad le permite dar seguimiento al consumo máximo de alimentación del sistema (el chasis y los módulos) registrado durante un periodo de tiempo. Haga clic en la subficha Configuración en la página Estado del presupuesto para borrar este valor. El valor para el consumo máximo de alimentación del sistema se indica en vatios y en BTU/h.
Fecha y hora de inicio del consumo máximo de alimentación del sistema	Muestra la fecha y la hora registrados cuando se borró por última vez el valor de consumo máximo de alimentación del sistema. La fecha y hora aparecen en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer las estadísticas de del consumo de alimentación máximo/mínimo y también cuando se restablece o falla el CMC.
Fecha y hora del consumo máximo de alimentación del sistema	Muestra la fecha y la hora registradas cuando se presentó el consumo máximo de alimentación del sistema durante el periodo registrado. La fecha y la hora aparecen en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día, 1-31 y AAAA es el año.
Consumo mínimo de alimentación del sistema	Muestra el valor del nivel de consumo mínimo de corriente alterna en el sistema (en vatios) en el tiempo desde la última vez que el usuario borró este valor. Esta propiedad permite seguir de cerca el consumo mínimo de alimentación del sistema (el chasis y los módulos) que se ha registrado a lo largo de un periodo de tiempo. Haga clic en la subficha Configuración en la página Estado del presupuesto para borrar este valor. El valor para el consumo mínimo de alimentación del sistema se indica en vatios y en BTU/h. Este valor se restablece con el botón Restablecer las estadísticas de del consumo de alimentación máximo/mínimo y también cuando se restablece o falla el CMC.
Fecha y hora de inicio del consumo mínimo de alimentación del sistema	Muestra la fecha y la hora registrados cuando se borró por última vez el valor de consumo mínimo de alimentación del sistema. La fecha y hora aparecen en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer las estadísticas de del consumo de alimentación máximo/mínimo y también cuando se restablece o falla el CMC.
Fecha y hora del consumo mínimo de alimentación del sistema	Muestra la fecha y hora registradas cuando se presentó el consumo mínimo de alimentación del sistema durante el periodo registrado. El formato de la fecha y hora es el mismo que el descrito para Fecha y hora del consumo máximo de alimentación del sistema .
Alimentación inactiva del sistema	Muestra el consumo de alimentación estimado del chasis cuando está en estado inactivo. El estado inactivo se define como el estado del chasis mientras está encendido y todos los módulos consumen energía mientras está en estado inactivo. Es un valor estimado y no cuantificado. Se computa como la alimentación acumulada asignada a los componentes de la infraestructura del chasis (módulos de E/S, ventiladores, iKVM, controladores de iDRAC y LCD del panel anterior) con un requerimiento mínimo de alimentación de todos los servidores a los que se asignó alimentación y están encendidos. El valor para la alimentación inactiva del sistema se indica en vatios y en BTU/h.
Alimentación potencial del sistema	Muestra el consumo estimado de alimentación del chasis cuando funciona con la máxima alimentación. El consumo máximo de alimentación se define como el estado del chasis cuando está encendido y todos los módulos consumen alimentación máxima. Es un valor estimado y no cuantificado. Se computa como la alimentación acumulada asignada a los componentes de la infraestructura del chasis (módulos de E/S, ventiladores, iKVM, controladores de iDRAC y LCD del panel anterior) con un requerimiento máximo de alimentación de todos los servidores a los que se asignó alimentación y están encendidos. El valor para la alimentación potencial del sistema se indica en vatios y en BTU/h.
Lectura de la corriente de entrada del sistema	Muestra el consumo de corriente de entrada total del chasis de acuerdo a la suma del consumo de corriente de entrada de cada uno de los módulos de las unidades de suministro de consumo individuales en el chasis. El valor de la lectura de la corriente de entrada del sistema se muestra en amperios.

Tabla 8-6. Estado de las estadísticas de alimentación de tiempo real

N.º	Descripción
Consumo de energía del sistema	Indica el consumo acumulado actual de energía de todos los módulos en el chasis medido desde la entrada de los suministros de energía. El valor se muestra en kilovatios por hora y es un valor acumulativo.

Fecha y hora de inicio de la energía del sistema	Muestra la fecha y la hora registrados cuando se borró por última vez el valor de consumo de energía del sistema, y comenzó el nuevo ciclo de mediciones. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer estadísticas de energía , pero persistirá a lo largo de las operaciones de reinicio o de transferencia de funciones ante fallas del CMC.
Fecha y hora del consumo de energía del sistema	Muestra la fecha y hora cuando se calculó el consumo de energía del sistema para mostrarlo. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año.

Tabla 8-7. Estado de la alimentación del sistema

N.º	Descripción
Condición general de la alimentación	Indica la condición (En buen estado , No crítico , Crítico , No recuperable , Otro , Desconocido) del subsistema de alimentación del chasis.
Estado de la alimentación del sistema	Muestra el estado de la alimentación (Encendido , Apagado , Encendiéndose , Apagándose) del chasis.
Redundancia	Indica el estado de redundancia. Los valores válidos son: No: las unidades de suministro de energía no son redundantes Sí: hay redundancia total

Tabla 8-8. Configuración de la política de alimentación del sistema

N.º	Descripción
Capacidad de alimentación de entrada del sistema	Indica el límite máximo de consumo de energía definido por el usuario para todo el sistema (el chasis, los CMC, los servidores, los módulos de E/S, las unidades de suministro de energía, el iKVM y los ventiladores). El CMC implementará este límite regulando la asignación de alimentación a los servidores o apagando los módulos de los servidores con menor prioridad. El valor para la capacidad de alimentación de entrada del sistema se muestra en vatios, BTU/h y porcentajes. Si el consumo de energía del chasis excede la Capacidad de alimentación de entrada del sistema , el rendimiento de los servidores con menor prioridad se reduce hasta que el consumo total de energía sea menor a la capacidad. En caso que se establezcan servidores con la misma prioridad, la selección del servidor para la reducción de la alimentación, o para la acción de apagado, se basa en el orden del número de ranura del servidor. Por ejemplo, el servidor en la ranura 1 se selecciona primero y el servidor en la ranura 16 se selecciona último.
Excedente por rendimiento máximo	El valor del excedente por rendimiento máximo es la diferencia entre la Capacidad de alimentación de entrada del sistema y la suma de la Alimentación de entrada máxima asignada a los servidores y la Alimentación de entrada máxima asignada a la infraestructura del chasis . El valor del excedente por rendimiento máximo se indica en vatios y en BTU/h.
Política de redundancia	Indica la configuración de redundancia actual: Redundancia de CA , Redundancia de suministro de energía y Sin redundancia . Redundancia de CA: la carga de la entrada de la alimentación está balanceada a lo largo de todas las unidades de suministro de energía. Tres de las unidades de suministro de energía están conectadas a una red de CA y las otras tres están conectadas a otra red. Cuando el sistema funciona de manera óptima en el modo Redundancia de CA, la carga de la alimentación se distribuye entre todos los suministros activos. En caso de una falla de la red, las unidades de suministro de energía en la red de CA que está funcionando toman el control al 100% de la capacidad. NOTA: En el modo Redundancia de CA, una diferencia en el número de unidades de suministro de energía entre los dos circuitos CA (por ejemplo, tres unidades de suministro de energía en un circuito de CA y dos en el otro circuito) provocará una degradación de la redundancia del sistema. Redundancia del suministro de energía: la capacidad de la unidad de suministro de energía con la clasificación más alta en el chasis se mantiene como repuesto, para asegurar que una falla de cualquiera de las unidades de suministro de energía no ocasione que los módulos de servidor o el chasis se apaguen. El modo Redundancia del suministro de energía no utiliza las seis unidades de suministro de energía; usa un máximo de cuatro. Las unidades de suministro de energía excedentes de cuatro no participan en la Redundancia del suministro de energía a menos que una unidad de suministro de energía falle o se desmonte. Sin redundancia: la energía de las tres unidades de suministro de energía en un circuito de CA (red) se usa para alimentar a todo el chasis, incluyendo el chasis, los servidores, los módulos de E/S, el iKVM y el CMC. AVISO: El modo Sin redundancia utiliza sólo tres unidades de suministro de energía al mismo tiempo, sin unidades de respaldo. La falla de una de las tres unidades de suministro de energía en uso podría ocasionar que los módulos de servidor pierdan energía y datos.
Acoplamiento dinámico del suministro de energía	Indica si Acoplamiento dinámico del suministro de energía está activado o desactivado. La activación de esta función permite al CMC colocar a las unidades de suministro de energía subutilizadas en modo de espera, dependiendo de la política de redundancia establecida y de los requisitos de alimentación del sistema. Al colocar a las unidades de suministro de energía subutilizadas en modo de espera, se incrementa la utilización y la eficacia de las unidades de suministro de energía en línea, lo que ahorra energía.

Tabla 8-9. Presupuesto de alimentación

--	--

N.º	Descripción
Capacidad máx. de alimentación de entrada del sistema	Máxima alimentación de entrada que los suministros de energía disponibles pueden proporcionarle al sistema (en vatios).
Reserva de redundancia de entrada	Muestra la cantidad de alimentación redundante (en vatios) en reserva que se puede usar en caso de falla de la red de CA o de una unidad de suministro de energía. Cuando el chasis se configura para funcionar en modo de Redundancia de CA , la Reserva de redundancia de entrada es la cantidad de energía de reserva que se puede utilizar en caso de falla de la red de CA. Cuando el chasis se configura para funcionar en modo de Redundancia de suministro de energía , la Reserva de redundancia de entrada es la cantidad de alimentación de reserva que se puede utilizar en caso de falla de una unidad específica de suministro de energía.
Alimentación de entrada asignada a los servidores	Muestra (en vatios) la alimentación de entrada acumulada que el CMC asigna a los servidores de acuerdo a su configuración.
Alimentación de entrada asignada a la infraestructura de chasis	Muestra (en vatios) la alimentación de entrada acumulada que el CMC asigna a la infraestructura del chasis (ventiladores, módulos de E/S, iKVM, CMC, CMC en espera, e iDRAC en servidores).
Alimentación total de entrada disponible para asignar	Indica el presupuesto de alimentación total del chasis, en vatios, que está disponible para la operación del chasis.
Capacidad de alimentación de entrada en espera	Muestra la cantidad de alimentación de entrada en espera (en vatios) disponible en el caso de una falla en el suministro de energía o un desmonte del suministro de energía del sistema. Es posible que este campo muestre lecturas cuando el sistema tenga cuatro o más suministros de energía y el acoplamiento dinámico del suministro de energía esté activado. NOTA: Es posible ver una unidad de suministro de energía modo de espera pero no contribuir al valor capacidad de alimentación de entrada en espera. En este caso, los vatios de esta unidad de suministro de energía contribuyen al valor Alimentación total de entrada disponible para asignar .

Tabla 8-10. Módulos de servidor

N.º	Descripción
Nº de ranura	Muestra la ubicación del servidor en el módulo del servidor. El Nº de ranura es un número en secuencia (1 a 16) que identifica el módulo de servidor por su ubicación dentro del chasis.
Nombre	Muestra el nombre del servidor. El usuario puede redefinir el nombre del servidor.
Tipo	Muestra el tipo del servidor.
Prioridad	Indica el nivel de prioridad asignado a la ranura del servidor en el chasis para elaborar el presupuesto de alimentación. El CMC usa este valor en sus cálculos cuando la alimentación se debe reducir o reasignar dependiendo de los límites de la alimentación definidos por el usuario o debido a fallas del suministro de energía o de la red de alimentación. Niveles de prioridad: 1 (la mayor) a 9 (la menor) Valor predeterminado: 1 NOTA: El nivel de prioridad de la ranura del servidor está asociado con la ranura del servidor, no con el servidor insertado en la ranura. Si un servidor se mueve a una ranura diferente en el chasis o a otro chasis, la prioridad asociada anteriormente con la nueva ranura determina la prioridad del servidor reubicado.
Estado de la alimentación	Muestra el estado de alimentación del servidor: <ul style="list-style-type: none"> o N/A: el CMC no ha determinado el estado de la alimentación del servidor. o Apagado: el servidor o el chasis están apagados. o Encendido: tanto el chasis como el servidor están encendidos. o Encendiendo: estado temporal entre apagado y encendido. Cuando se completa el ciclo de encendido, el estado de la alimentación cambiará a Encendido. o Apagando: estado temporal entre Encendido y Apagado. Cuando se completa el ciclo de apagado, el estado de la alimentación cambiará a Apagado.
Asignación de presupuesto	Muestra la cantidad asignada de presupuesto de alimentación para el módulo de servidor.

Tabla 8-11. Suministros de energía del sistema

N.º	Descripción
Nombre	Muestra el nombre de la unidad de suministro de energía en el formato PS- <i>n</i> , donde <i>n</i> es el número de la unidad de suministro de energía.
Estado de la alimentación	Indica el estado de la alimentación de la unidad de suministro de energía: Encendido , Inicializando , En línea , En espera , En diagnóstico , Fallido , Redundante , Desconocido o Ausente (perdido).
Voltios de entrada	Muestra el voltaje de entrada actual del suministro de energía.

Corriente de entrada	Muestra la corriente de entrada actual del suministro de energía.
Alimentación clasificada de salida	Muestra la máxima clasificación de alimentación de salida del suministro de energía.

Configuración de redundancia de alimentación y consumo máximo

El servicio de administración de la alimentación del CMC optimiza el consumo de alimentación para todo el chasis (el chasis, los servidores, los módulos de E/S, el iKVM, el CMC y las unidades de suministro de energía) y reasigna la alimentación a diferentes módulos en función de la demanda.

Por medio de la interfaz web

 **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

1. **Inicie sesión en la interfaz web del CMC.**
2. Seleccione **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Se muestra la página **Power Budget Status (Estado de consumo máximo)**.
4. Haga clic en la subficha **Configuration (Configuración)**. Se muestra la página **Budget/Redundancy Configuration (Configuración de redundancia de alimentación/consumo máximo)**.
5. Establezca cualquiera o todas las propiedades descritas en la [tabla 8-12](#) según sus necesidades.
6. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Para actualizar el contenido de la página **Configuración de redundancia/presupuesto**, haga clic en **Actualizar**. Para imprimir el contenido, haga clic en **Imprimir**.

Tabla 8-12. Propiedades configurables del presupuesto de alimentación/redundancia

N.º	Descripción
Excedente por rendimiento máximo	El valor del excedente por rendimiento máximo es la diferencia entre la Capacidad de alimentación de entrada del sistema y la Alimentación requerida para el rendimiento máximo (suma de la Alimentación de entrada máxima asignada a los servidores y la Alimentación de entrada máxima asignada a la infraestructura del chasis). El valor del excedente por rendimiento máximo se indica en vatios y en BTU/h.
Alimentación requerida para el rendimiento máximo	El valor de la alimentación requerida para el rendimiento máximo es la suma de la Necesidad de alimentación de entrada máxima de los servidores que se encienden y la Alimentación de entrada asignada a la infraestructura de chasis . El valor de la alimentación requerida para el rendimiento máximo se indica en vatios y en BTU/h. Si la Capacidad de alimentación de entrada del sistema se configura menor a la Alimentación requerida para el rendimiento máximo , es posible que algunos servidores se regulen bajo una carga extrema.
Capacidad de alimentación de entrada del sistema	<p>La capacidad de alimentación de entrada del sistema es la alimentación máxima de CA que el sistema puede asignar a los servidores y a la infraestructura del chasis. La puede configurar el usuario en cualquier valor que exceda la alimentación mínima necesaria para que se enciendan los servidores y para la infraestructura del chasis. Si se configura un valor menor a la alimentación mínima necesaria para los servidores y la infraestructura del chasis, éste fallará.</p> <p>La alimentación asignada a los servidores y a la infraestructura del chasis puede encontrarse en la interfaz del usuario en la página de estado Chasis -> Administración de la alimentación-> Presupuesto de alimentación debajo de la sección Presupuesto de alimentación o a través del comando de utilidades de CLI RACADM (<code>racadm getpbinfo</code>).</p> <p>Los usuarios pueden APAGAR uno o más servidores para disminuir la asignación actual de alimentación e intentar configurar otra vez un valor menor para la Capacidad de alimentación de entrada del sistema (si así se desea) o simplemente para configurar la capacidad antes de encender los servidores.</p> <p>Para cambiar esta configuración, se puede introducir un valor en cualquiera de las unidades. La interfaz asegura que el campo de unidades que se cambió por última vez será el valor que se envíe cuando se apliquen los cambios.</p> <p>NOTA: Consulte la herramienta Datacenter Capacity Planner (DCCP) en www.dell.com/calc para obtener información sobre la planificación de la capacidad.</p> <p>NOTA: Cuando los cambios de los valores se especifican en vatios, el valor enviado reflejará exactamente lo que se aplica en realidad. Sin embargo, cuando los cambios se envían en BTU/h o porcentajes, el valor enviado no reflejará exactamente lo que se aplica en realidad. Esto se debe a que las unidades son convertidas a vatios y luego aplicadas; y es posible que la conversión sea susceptible a errores de redondeo.</p>
Política de redundancia	<p>Esta opción le permitirá seleccionar una de las siguientes opciones:</p> <ul style="list-style-type: none"> ○ Sin redundancia: la energía de los tres suministros de energía en un circuito de CA (red) se usa para alimentar a todo el chasis, incluyendo el chasis, los servidores, los módulos de E/S, el iKVM y el CMC.

	<p>NOTA: El modo Sin redundancia utiliza sólo tres suministros de energía al mismo tiempo. Si hay 3 unidades de suministro de energía instaladas, no habrá ninguna unidad de respaldo disponible. La falla de uno de los tres suministros de energía podría causar la pérdida de energía y/o datos por parte de los servidores. Si las unidades de suministro de energía 4-6 están presentes, serán redundantes y estarán disponibles en caso de que una unidad de suministro de energía en línea disminuya.</p> <ul style="list-style-type: none"> ○ Redundancia del suministro de energía: la capacidad del suministro de energía con la clasificación más alta en el chasis se mantiene como repuesto, para asegurar que una falla de cualquier suministro de energía no ocasione que los módulos de servidor o el chasis se apaguen (reserva en caliente). <p>Redundancia del suministro de energía no utiliza los seis suministros de energía, sino un máximo de cuatro y mínimo de dos suministros de energía. Redundancia del suministro de energía evita que los módulos de servidor se enciendan si el consumo de la alimentación del chasis excede la alimentación clasificada. La falla de dos suministros de energía podría ocasionar que se apaguen todos o algunos de los módulos del servidor en el chasis. Los módulos del servidor no se regulan en este modo.</p> <ul style="list-style-type: none"> ○ Redundancia de CA: este modo divide las 6 unidades de suministro de energía en dos redes (las unidades de suministro de energía 1-3 conforman la red 1 y las unidades de suministro de energía 4-6 conforman la red 2). Se requieren 6 unidades de suministro de energía para tener una política de alimentación de Redundancia de CA totalmente redundante. En esta configuración, 3 unidades de suministro de energía en una red estarán en línea y 3 unidades de suministro de energía en la otra red serán redundantes. La transferencia por falla ocurrirá cuando falle alguna de las 3 unidades de suministro de energía en la red en línea, lo que provocará que las unidades de suministro de energía redundantes estén en línea e informen como degradada la política de redundancia. <p>NOTA: En el modo Redundancia de CA, una diferencia en el número de unidades de suministro de energía entre los dos circuitos CA (por ejemplo, tres suministros de energía en un circuito de CA y dos en el otro circuito) provocará una degradación de la redundancia.</p>
<p>Activar el acoplamiento dinámico del suministro de energía</p>	<p>Activa (cuando está verificada) la administración dinámica de la alimentación. En el modo Acoplamiento dinámico, los suministros de energía se Encienden o Apagan según el consumo de energía, lo que optimiza el consumo de energía de todo el chasis.</p> <p>Por ejemplo, usted tiene presupuesto de alimentación de 5000 vatios, la política de redundancia está configurada en modo de redundancia de CA, y cuenta con seis unidades de suministro de energía. El CMC determina que cuatro unidades de suministro de energía pueden administrar la redundancia de CA mientras que las otras dos permanecen en modo de espera. Si se requiere una alimentación adicional de 2000 vatios para servidores instalados recientemente, se acoplan las dos unidades de suministro de energía en espera.</p>
<p>Desactivar botón de encendido del chasis</p>	<p>Cuando se selecciona, desactiva el botón de alimentación del chasis. Si se selecciona la casilla de marcación y el usuario intenta cambiar el estado de la alimentación del chasis mediante el botón de alimentación del chasis, la acción del usuario se ignorará.</p>

Uso de RACADM

Para activar la redundancia y establecer la política de redundancia:

 **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.
2. Establezca las propiedades según sea necesario:

- 1 Para establecer el presupuesto de alimentación máximo para el chasis, escriba:

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <valor>
```

donde <valor> es un número entre 2768 y 7928 que representa el límite máximo de la alimentación en vatios. El valor predeterminado es 7928.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgChassisPower -o cfgChassisInMaxPowerCapacity 5400
```

establece el presupuesto de alimentación máximo en 5400 vatios.

- 1 Para seleccionar una política de redundancia, escriba:

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <valor>
```

donde <valor> es **0** (Sin redundancia), **1** (Redundancia de CA), **2** (Suministro de energía redundante). El valor predeterminado es 0.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

establece la política de redundancia en 1.

- 1 Para activar o desactivar el acoplamiento dinámico de las unidades de suministro de energía, escriba:

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <valor>
```

donde <valor> es **0** (desactivar), **1** (activar). El valor predeterminado es 1.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```

desactiva el acoplamiento dinámico de las unidades de suministro de energía.

Para obtener información acerca de los comandos de RACADM para la alimentación del chasis:

- 1 Consulte el apartado [config](#).
- 1 Consulte el apartado [getconfig](#).
- 1 Consulte el apartado [getobjinfo](#).
- 1 Consulte el apartado [cfgChassisPower](#).

Asignación de niveles de prioridad a los servidores

Los niveles de prioridad de servidor determinan de qué servidores obtiene energía la CMC cuando se necesita energía adicional.

-  **NOTA:** La prioridad que asigna a un servidor está vinculada a su ranura y no al servidor. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad desde la nueva ubicación.
-  **NOTA:** Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control de chasis**.

Por medio de la interfaz web

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Servers (Servidores)** en el árbol del sistema. Aparece la página **Servers Status (Estado de servidores)**.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Aparece la página **Server Priority (Prioridad de servidores)**, en la que se muestra una lista de todos los servidores del chasis.
4. Seleccione un nivel de prioridad (de 1 a 9, siendo 1 la prioridad máxima) para uno, varios o todos los servidores. El valor predeterminado es 1. Puede asignar el mismo nivel de prioridad a varios servidores.
5. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <número de ranura> <nivel de prioridad>
```

Donde *<número de ranura>* (1 a 16) se refiere a la ubicación del servidor y *<nivel de prioridad>* es un valor entre 1 y 9.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

establece el nivel de prioridad en 1 para el servidor con el nombre de índice de 5.

Establecimiento del presupuesto de alimentación

-  **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

Por medio de la interfaz web

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema. Aparecerá la página **Estado del componente**.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Aparece la página **Power Budget Status (Estado de consumo máximo)**.
4. Haga clic en la subficha **Configuration (Configuración)**. Aparece la página **Budget/Redundancy Configuration (Configuración de redundancia de alimentación y consumo máximo)**.
5. Escriba un valor del presupuesto de hasta 7928 vatios en el campo de texto **Capacidad de alimentación de entrada del sistema**.

-  **NOTA:** El consumo máximo se limita a tres PSU como máximo de un total de seis. Si intenta definir un valor de consumo máximo de energía CA que sobrepase la capacidad de alimentación del chasis, la CMC mostrará un mensaje de error.
-  **NOTA:** Cuando los cambios de los valores se especifican en vatios, el valor enviado reflejará exactamente lo que se aplica en realidad. Sin embargo, cuando los cambios se envían en BTU/h o porcentajes, el valor enviado no reflejará exactamente lo que se aplica en realidad. Esto se debe a que las unidades son convertidas a vatios y luego aplicadas; y es posible que la conversión sea susceptible a errores de redondeo.

6. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgChassisPowerCap -o cfgChassisInMaxPowerCapacity <valor>
```

donde <valor> es la cantidad máxima de alimentación (en vatios) disponible para el chasis.

-  **NOTA:** El consumo máximo se limita a tres PSU como máximo de un total de seis. Si intenta definir un valor de consumo máximo de energía CA que sobrepase la capacidad de alimentación del chasis, la CMC mostrará un mensaje de error.

Por ejemplo,

```
racadm config -g cfgChassisPowerCap -o cfgChassisInMaxPowerCapacity 7928
```

Regulación de la alimentación para mantener el presupuesto de alimentación

El CMC regula la alimentación para los servidores con menor prioridad cuando se necesita alimentación adicional para mantener el límite máximo de alimentación de CA. Por ejemplo, cuando se acopla un nuevo servidor, el CMC podría reducir la alimentación de los servidores con menor prioridad para obtener más alimentación para el nuevo servidor. Si la cantidad de alimentación aún no es suficiente después de regular los servidores con menor prioridad, el CMC regula los servidores con mayor prioridad hasta que se libera suficiente energía para alimentar el nuevo servidor.

La regulación se ejecuta en dos casos:

- 1 El consumo de alimentación general excede el límite máximo de alimentación configurable (consulte [Establecimiento del presupuesto de alimentación](#))
- 1 Se produce una falla de alimentación en una configuración sin redundancia

Para obtener información sobre la asignación de niveles de prioridad a los servidores, consulte [Ejecución de operaciones de control de alimentación en el chasis](#).

Ejecución de operaciones de control de alimentación en el chasis

-  **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.
-  **NOTA:** Las operaciones de control de alimentación afectan a todo el chasis. En el caso de las operaciones de control de alimentación en un módulo de E/S, consulte [Ejecución de las operaciones de control de alimentación en un módulo de E/S](#). En el caso de las operaciones de control de alimentación en servidores, consulte [Ejecución de operaciones de control de alimentación en un servidor](#).

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación -como un apagado ordenado- en todo el chasis (el chasis, los servidores, los módulos de E/S, el iKVM y las unidades de suministro de energía).

Por medio de la interfaz web

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Se muestra la página **Power Budget Status (Estado de consumo máximo)**.
4. Haga clic en la subficha **Control**. Se muestra la página **Power Management (Administración de energía)**.
5. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
 - 1 **Encender el sistema:** enciende el sistema (equivalente a pulsar el botón de encendido cuando el chasis está **Apagado**). Esta acción se desactivará si el servidor ya está **Encendido**.
 -  **NOTA:** Esta opción enciende el chasis y otros subsistemas (el iDRAC en los servidores, los módulos de E/S y el iKVM). Los servidores no se encenderán.
 - 1 **Apagar el sistema:** apaga la alimentación del chasis. Esta acción se desactivará si el chasis ya está **Apagado**.

 **NOTA:** Esta acción apaga el chasis (chasis, servidores, módulos de E/S, iKVM y suministros de energía). Los CMC permanecen encendidos, pero en un estado de espera virtual; una unidad de suministro de energía y ventiladores enfrían a los CMC en este estado. El suministro de energía también proporcionará alimentación a los ventiladores que funcionarán a una velocidad baja.

- 1 **Ciclo de encendido del sistema (inicio en frío):** apaga el sistema y luego lo reinicia (inicio en frío). Esta acción se desactivará si el chasis ya está Apagado.

 **NOTA:** Esta acción apaga y luego reinicia el chasis completo (chasis, servidores configurados para estar siempre encendidos, módulos de E/S, iKVM y suministros de energía).

- 1 **Restablecer el CMC:** restablece el CMC sin apagarlo (reinicio mediante sistema operativo). Esta opción se desactiva si el CMC ya está apagado.

 **NOTA:** Esta acción sólo restablece el CMC. No se afecta a ningún otro componente.

- 1 **Apagado no ordenado:** esta acción impulsa un apagado no ordenado de todo el chasis (chasis, servidores, módulos de E/S, iKVM y suministros de energía). No intenta cerrar de forma ordenada el sistema operativo de los servidores antes de apagarlo.

6. Haga clic en **Aplicar**. Aparece un cuadro de diálogo que le solicita confirmación.

7. Haga clic en **OK (Aceptar)** para realizar la acción de administración de energía (por ejemplo, hacer que se reinicie el sistema).

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm chassisaction -m chassis <acción>
```

donde <acción> es encendido, apagado, ciclo de encendido, apagado no ordenado o reinicio.

Ejecución de las operaciones de control de alimentación en un módulo de E/S

Usted puede ejecutar de manera remota un restablecimiento o un ciclo de encendido en un módulo de E/S individual.

 **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

Por medio de la interfaz web

1. **Inicie sesión en la interfaz web del CMC.**
2. Seleccione **I/O Modules (Módulos de E/S)**. Se muestra la página **I/O Modules Status (Estado de módulos de E/S)**.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Se muestra la página **Power Control (Control de alimentación)**.
4. Seleccione la operación que desea ejecutar (reinicio o ciclo de encendido) en el menú desplegable que se encuentra junto al módulo de E/S en la lista.
5. Haga clic en **Aplicar**. Aparece un cuadro de diálogo que le solicita confirmación.
6. Haga clic en **Aceptar** para realizar la acción de administración de alimentación (por ejemplo, hacer que el módulo de E/S realice un ciclo de encendido).

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm chassisaction -m switch-<n> <acción>
```

donde <n> es un número de 1 a 6 y especifica el módulo de E/S (a1, a2, b1, b2, c1, c2), y <acción> indica la operación que desea ejecutar: ciclo de encendido o reinicio.

Ejecución de operaciones de control de alimentación en un servidor

 **NOTA:** Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación, por ejemplo, un apagado ordenado, en un servidor individual en el chasis.

Por medio de la interfaz web

1. **Inicie sesión en la interfaz web del CMC.**
2. Expanda **Servers (Servidores)** en el árbol del sistema y, a continuación, seleccione el servidor en el que desee ejecutar una operación de control de alimentación. Se muestra la página **Server Status (Estado de servidor)**.
3. Haga clic en la ficha **Power Management (Administración de energía)**. Se muestra la página **Server Power Management (Administración de energía del servidor)**.
4. **Estado de alimentación** muestra el estado de alimentación del servidor (uno de los siguientes):
 - 1 **N/A:** el CMC no ha determinado aún el estado de la alimentación del servidor.
 - 1 **Apagado:** el servidor o el chasis están apagados.
 - 1 **Encendido:** tanto el chasis como el servidor están encendidos.
 - 1 **Encendiendo:** estado temporal entre Apagado y Encendido. Cuando la acción de finaliza satisfactoriamente, el **Estado de la alimentación** será **Encendido**.
 - 1 **Apagando:** estado temporal entre Encendido y Apagado. Cuando la acción de finaliza satisfactoriamente, el **Estado de la alimentación** será **Apagado**.
5. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
 - 1 **Encender el servidor:** enciende el servidor (equivalente a pulsar el botón de encendido cuando el servidor está apagado). Esta acción se desactivará si el servidor ya está encendido.
 - 1 **Apagar el servidor:** apaga el servidor (equivalente a pulsar el botón de apagado cuando el servidor está encendido).
 - 1 **Apagado ordenado:** apaga y luego reinicia el servidor.
 - 1 **Restablecer el sistema (reinicio en caliente):** reinicia el servidor sin apagarlo. Esta opción se desactiva cuando el servidor ya está apagado.
 - 1 **Servidor del ciclo de encendido (reinicio en frío):** apaga el servidor y luego lo reinicia. Esta opción se desactiva cuando el servidor ya está apagado.
6. Haga clic en **Aplicar**. Aparece un cuadro de diálogo que le solicita confirmación.
7. Haga clic en **OK (Aceptar)** para realizar la acción de administración de energía (por ejemplo, hacer que se reinicie el servidor).

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm serveraction -m <módulo> <acción>
```

donde <módulo> especifica el servidor por su número de ranura (servidor 1 a 16) en el chasis y <acción> indica la operación que desea ejecutar: powerup, powerdown, powercycle, graceshutdown, or hardreset (encendido, apagado, ciclo de encendido, apagado ordenado o reinicio completo).

[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

- [Uso de una consola telnet o serie](#)
- [Uso de RACADM](#)
- [Uso de RACADM para configurar el CMC](#)
- [Configuración de las propiedades de red del CMC](#)
- [Uso de RACADM para configurar usuarios](#)
- [Configuración de alertas por correo electrónico y de SNMP](#)
- [Configuración de múltiples CMC en varios chasis](#)
- [Solución de problemas](#)
- [Actualizaciones de comandos para CMC 1.20](#)

RACADM proporciona un conjunto de comandos que le permiten configurar y administrar el CMC mediante una interfaz basada en texto. Se puede acceder a RACADM por medio de una consola de Telnet/SSH o una conexión serie, a través de la consola del CMC de Dell en el iKVM o de manera remota por medio la interfaz de línea de comandos de RACADM instalada en una estación de administración.

La interfaz de RACADM se clasifica como "local" o "remota", según de la ubicación del programa `racadm` ejecutable que se esté utilizando:

 **NOTA:** RACADM remoto se incluye en el *DVD Dell Systems Management Tools and Documentation* y se instala en una estación de administración.

- 1 RACADM remoto: usted ejecuta comandos de RACADM en una estación de administración con la opción `-r` y el nombre DNS o la dirección IP del CMC.
- 1 RACADM local: usted inicia sesión en el CMC por medio de Telnet, SSH, una conexión serie o el iKVM. Con RACADM local, está ejecutando la implementación de RACADM que es parte del firmware del CMC.

Puede utilizar comandos de RACADM remoto en secuencias de comandos para configurar varios CMC. El CMC no admite las secuencias de comandos, por lo que no puede ejecutar secuencias de comandos directamente en el CMC. Para obtener más información acerca de cómo configurar varios CMC, consulte [Configuración de múltiples CMC en varios chasis](#).

Esta sección ofrece la siguiente información:

- 1 El uso de los comandos `serie` y `racadm`. Consulte [Uso de una consola telnet o serie](#) o [Uso de RACADM](#).
- 1 Configuración del CMC por medio de RACADM. Consulte el apartado [Uso de RACADM para configurar el CMC](#).
- 1 Uso del archivo de configuración de RACADM para configurar varios CMC. Consulte el apartado [Configuración de múltiples CMC en varios chasis](#).

Uso de una consola telnet o serie

Puede iniciar sesión en el CMC ya sea mediante una conexión serie o Telnet/SSH, o por medio de la consola del CMC de Dell en el iKVM. Para configurar el CMC para el acceso serie o remoto, consulte [Configuración del CMC para el uso de consolas de línea de comandos](#). Las opciones de subcomandos de uso más frecuente se describen en [tabla 4-2](#). Hay una lista completa de subcomandos de RACADM en [Subcomandos de RACADM](#).

Inicio de sesión en el CMC

Una vez que se ha configurado el software del emulador de terminal de la estación de administración y el BIOS del nodo administrado, realice los pasos siguientes para iniciar sesión en el CMC:

1. Inicie sesión en el CMC con el software de emulación de terminal de la estación de administración.
2. Escriba su nombre de usuario y contraseña para el CMC, y luego oprima <Entrar>.

Ahora está conectado al CMC.

Inicio de una consola de texto

Puede iniciar sesión en el CMC usando Telnet o SSH mediante una red, un puerto serie o la consola de CMC de Dell a través del iKVM. Abra una sesión de Telnet o de SSH, conéctese e inicie sesión en el CMC.

Para obtener información acerca de cómo conectarse al CMC a través del iKVM, consulte [Uso del módulo iKVM](#).

Uso de RACADM

Los subcomandos de RACADM se pueden ejecutar de manera remota desde la petición de comando de la consola serie o Telnet o por medio de una petición de comando normal.

Use los subcomandos de RACADM para configurar las propiedades del CMC y realizar tareas de administración de manera remota. Para ver una lista de

subcomandos de RACADM, escriba:

```
racadm help
```

Cuando se ejecuta sin opciones ni subcomandos, RACADM muestra información de la sintaxis e instrucciones para acceder a los subcomandos y a la ayuda. Para ver una lista de las opciones de sintaxis y de la línea de comandos para subcomandos individuales, escriba:

```
racadm help <subcomando>
```

Subcomandos de RACADM

[Tabla 4-1](#) proporciona una lista breve de subcomandos comunes que se utilizan en RACADM. Para ver una lista completa de los subcomandos de RACADM, incluso la sintaxis y las anotaciones válidas, consulte [Subcomandos de RACADM](#).

 **NOTA:** Los comandos para conectar, salir, cerrar y desconectar son comandos integrados del CMC, no comandos de RACADM. No se pueden utilizar con RACADM remoto. Consulte [Conexión a módulos por medio del comando connect](#) para obtener información sobre el uso de estos comandos.

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

```
racadm help
```

Tabla 4-1. Subcomandos de RACADM

Comando	Descripción
help	Muestra las descripciones de los subcomandos del CMC.
help <subcomando>	Muestra el resumen sobre el uso del subcomando especificado.
?	Muestra las descripciones de los subcomandos del CMC.
? <subcomando>	Muestra el resumen sobre el uso del subcomando especificado.
arp	Muestra el contenido de la tabla de ARP. Las anotaciones del ARP no se pueden agregar ni eliminar.
chassisaction	Ejecuta el encendido, el apagado, el restablecimiento y el ciclo de encendido en el chasis, el conmutador y el KVM.
clrraclog	Borra el registro del CMC y crea una sola anotación indicando el usuario y la hora a la que se borró el registro.
clrsel	Borra las anotaciones del registro de sucesos del sistema.
cmchangeover	Cambia el estado del CMC de activo a modo de espera, o viceversa, en entornos de CMC redundantes.
config	Configura el CMC.
deploy	Instala un servidor mediante la especificación de las propiedades requeridas.
feature	Muestra las funciones activadas y la desactivación de las funciones.
featurecard	Muestra información del estado de la tarjeta de función.
fwupdate	Realiza actualizaciones de firmware de los componentes del sistema, y muestra el estado de actualización del firmware.
getassettag	Muestra la etiqueta de propiedad del chasis.
getchassisname	Muestra el nombre del chasis.
getconfig	Muestra las propiedades de configuración actuales del CMC.
getdcinfo	Muestra información general de configuración errónea del módulo de E/S y de la tarjeta subordinada.
getflexaddr	Muestra el estado activado/desactivado de FlexAddress por ranura/estructura de red. Si se usa con la opción -i, el comando muestra las direcciones WWN y MAC para una ranura en particular.
getioinfo	Muestra información general del módulo de E/S.
getkvminfo	Muestra información acerca del iKVM.
getled	Muestra la configuración de los LED en un módulo.
getmacaddress	Muestra la dirección MAC de un servidor.
getmodinfo	Muestra información de la configuración del módulo y del estado.
getniccfg	Muestra la configuración IP actual del controlador.
getpbinfo	Muestra información del estado del presupuesto de alimentación.
getraclog	Muestra el registro del CMC.
getractime	Muestra la hora del CMC.
getredundancymode	Muestra el modo de redundancia del CMC.
getsel	Muestra el registro de sucesos del sistema (registro de hardware).
getsensorinfo	Muestra información acerca de los sensores del sistema.
getslotname	Muestra el nombre de una ranura en el chasis.
getssninfo	Muestra información sobre las sesiones activas.
getsvctag	Muestra las etiquetas de servicio.
getsysinfo	Muestra información general del CMC y del sistema.
gettracelog (sólo para uso interno de Dell)	Muestra el registro de rastreo del CMC. Si se usa con la opción -i, el comando muestra el número de anotaciones en el registro de rastreo del CMC.

ifconfig	Muestra la configuración actual de IP del CMC.
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.
ping	Verifica que se pueda acceder a la dirección IP de destino desde el CMC con el contenido actual de la tabla de enrutamiento.
racdump	Muestra información completa del estado de configuración y del estado del chasis, así como también registros de sucesos históricos. Se usa para realizar una verificación de la configuración después de la instalación y durante las sesiones de depuración de errores.
racreset	Restablece el CMC.
racresetcfg	Restablece la configuración predeterminada del CMC.
serveraction	Realiza operaciones de administración de energía en el sistema administrado.
setassettag	Establece la etiqueta de propiedad del chasis.
setchassisname	Establece el nombre del chasis.
setflexaddr	Activa/desactiva FlexAddress en una ranura/estructura de red en particular, cuando la función FlexAddress está activada en el chasis.
setled	Establece la configuración de los indicadores LED de un módulo.
setniccfg	Establece la configuración IP para el controlador.
setractime	Establece la hora del CMC.
setslotname	Establece el nombre de una ranura en el chasis.
setsysinfo	Establece el nombre y la ubicación del chasis.
sslcertdownload	Descarga un certificado firmado por una autoridad de certificados.
sslcertupload	Carga un certificado firmado por una autoridad de certificados o un certificado de servidor para el CMC.
sslcertview	Visualiza un certificado firmado por una autoridad de certificados o un certificado de servidor en el CMC.
sslcsrgen	Genera y descarga la CSR de SSL.
sslresetcfg	Genera nuevamente el certificado autofirmado utilizado por el CMC de Web GUI.
testemail	Obliga al CMC a enviar un correo electrónico a través del NIC del CMC.
testtrap	Obliga al CMC a enviar un SNMP a través del NIC del CMC.

Acceso a RACADM de manera remota

Tabla 4-2 muestra las opciones para los subcomandos de RACADM remoto.

Tabla 4-2. Opciones para los subcomandos de RACADM remoto

Opción	Descripción
-r <Direc_IP_del_RAC>	Especifica la dirección IP?remota del controlador.
-r <Direc_IP_del_RAC>:<puerto>	Use <número de puerto> si el número de puerto del CMC no es el puerto predeterminado (443)
-i	Indica a RACADM que solicite 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 la opción -i (interactiva) no se permite.
-p <contraseña>	Especifica la contraseña usada para autenticar la transacción del comando. Si se usa la opción -p, la opción -i no se permite.

Para acceder a la RACADM de manera remota, escriba los siguientes comandos:

```
racadm -r <dirección IP del CMC> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>
```

```
racadm -i -r <dirección IP del CMC> <subcomando> <opciones del subcomando>
```

 **NOTA:** La opción -i indica a la RACADM que solicite interactivamente el nombre de usuario y la contraseña. Sin la opción -i, usted debe proporcionar el nombre de usuario y la contraseña en el comando usando las opciones -u y -p.

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 CMC se ha cambiado a un puerto personalizado diferente al puerto predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP del CMC>:<puerto> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>
```

```
racadm -i -r <dirección IP del CMC>:<puerto> <subcomando> <opciones del subcomando>
```

Activación y desactivación de la capacidad remota de RACADM

 **NOTA:** Dell recomienda ejecutar estos comandos en el chasis.

La capacidad remota de RACADM está activada de manera predeterminada. En los siguientes comandos, **g** especifica el grupo de configuración al que pertenece el objeto y **-o** especifica el objeto de configuración que se va a configurar.

Para desactivar la capacidad remota de RACADM, escriba:

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

Para volver a activar la capacidad remota de RACADM, escriba:

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

Uso de RACADM de manera remota

 **NOTA:** Configure la dirección IP en el CMC antes de usar la capacidad remota de RACADM. Para obtener más información acerca de cómo configurar el CMC, consulte [Instalación y configuración del CMC](#).

La opción **remota** (-r) de la consola de RACADM le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para usar la capacidad remota, usted necesita un nombre de usuario válido (opción -u) y una contraseña (opción -p), así como la dirección IP del CMC.

Antes de intentar acceder a la RACADM de manera remota, confirme que tiene los permisos para hacerlo. Para ver sus privilegios de usuario, escriba:

```
racadm getconfig -g cfguseradmin -i n
```

donde *n* es su identificación de usuario (1 a 16).

Si no conoce su identificación de usuario, intente utilizando diferentes valores para *n*.

 **NOTA:** La capacidad remota de RACADM se admite sólo en estaciones de administración mediante un explorador admitido. Para obtener más información, consulte el apartado [Exploradores de web compatibles](#).

 **NOTA:** Cuando se usa la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas donde se van a usar los subcomandos de RACADM que involucren operaciones con archivos. Por ejemplo,

```
racadm getconfig -f <nombre de archivo> -r <dirección IP>
```

O bien:

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

Mensajes de error de RACADM

Para obtener información acerca de los mensajes de error de la CLI de RACADM, consulte [Solución de problemas](#).

Uso de RACADM para configurar el CMC

 **NOTA:** Para configurar el CMC por primera vez. Debe haber iniciado sesión como usuario **root** para ejecutar comandos de RACADM en un sistema remoto. Se puede crear otro usuario para otorgar permiso al mismo para configurar el CMC.

La interfaz web del CMC es la forma más rápida de configurar el CMC (consulte [Uso de la interfaz web del CMC](#)). Sin embargo, si prefiere la configuración de CLI o de secuencia de comandos, o si necesita configurar varios CMC, use RACADM, que se instala con los agentes del CMC en la estación de administración.

Configuración de las propiedades de red del CMC

Configuración del acceso inicial al CMC

Antes de que pueda comenzar a configurar el CMC, debe configurar primero los valores de red del CMC para permitir la administración del CMC de manera remota. Esta configuración inicial asigna los parámetros del sistema de red TCP/IP para permitir el acceso al CMC.

En esta sección se explica cómo realizar la configuración inicial de red del CMC por medio de los comandos de RACADM. Toda la configuración descrita en esta sección se puede realizar por medio de la pantalla LCD del panel anterior. Consulte el apartado [Configuración del sistema de red por medio del asistente de configuración del panel LCD](#).

 **AVISO:** Si cambia la configuración de red del CMC, podría provocar que su conexión de red actual se desconecte.

Para obtener más información sobre los subcomandos de red, consulte [Subcomandos de RACADM](#) y [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#).

 **NOTA:** Debe tener privilegios de **Administrador de configuración del chasis** para establecer la configuración de red del CMC.

De manera predeterminada, el CMC solicita y obtiene automáticamente una dirección IP del CMC a partir del servidor de protocolo de configuración dinámica de host (DHCP).

Puede desactivar esta función y especificar la dirección IP estática del CMC, la puerta de enlace y la máscara de subred.

Para desactivar el DHCP y especificar la dirección IP estática del CMC, la puerta de enlace y la máscara de subred, escriba:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgNicIpAddress <dirección IP estática>

racadm config -g cfgLanNetworking -o cfgNicGateway <puerta de enlace estática>

racadm config -g cfgLanNetworking -o cfgNicNetmask <máscara de subred estática>
```

Cómo ver la configuración de red actual

Para ver un resumen de la configuración del NIC, el DHCP, la velocidad de la red y dúplex, escriba:

```
racadm getniccfg
```

O bien:

```
racadm getconfig -g cfgCurrentLanNetworking
```

Para ver la dirección IP y DHCP, la dirección MAC y la información de DNS del chasis, escriba:

```
racadm getsysinfo
```

Configuración de los valores de red de la LAN

 **NOTA:** Para realizar los siguientes pasos, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Los valores de la LAN, como la cadena de comunidad y la dirección IP del servidor SMTP, afectan tanto al CMC como a la configuración externa del chasis.

 **NOTA:** Si tiene dos CMC (principal y en espera) en el chasis, y están conectados a la red, el CMC en espera automáticamente asumirá la configuración de la red en caso que el CMC principal falle.

Activación del NIC del CMC

Para activar el NIC del CMC, escriba:

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

 **NOTA:** El NIC del CMC está activado de manera predeterminada.

Activación o desactivación del DHCP para la dirección del NIC

Cuando está activada, la función de DHCP para la dirección del NIC del CMC solicita y obtiene automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP). Esta función está activada de manera predeterminada.

Usted puede desactivar la función de DHCP para la dirección del NIC y especificar una dirección IP estática, una máscara de subred y una puerta de enlace. Para obtener instrucciones, consulte [Configuración del acceso inicial al CMC](#).

 **NOTA:** Si desactiva la función de DHCP para la dirección del NIC y la reactiva posteriormente, la dirección IP estática, la máscara de subred y la puerta de enlace se perderán.

Activación o desactivación del DHCP para la dirección IP de DNS

De manera predeterminada, la función de DHCP para la dirección de DNS del CMC está desactivada. Cuando está activada, esta función obtiene las direcciones principal y secundaria del servidor DNS a partir del servidor DHCP. Usando esta función, usted no tiene que configurar direcciones IP estáticas para el servidor DNS.

Para desactivar la función de DHCP para la dirección de DNS y especificar direcciones estáticas del servidor DNS preferido y alternativo, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP
```

Establecimiento de direcciones IP estáticas de DNS

 **NOTA:** Estos valores no son válidos a menos que la función de DHCP para la dirección de DNS esté desactivada.

Para establecer la dirección IP de DNS preferida, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <dirección_IP>
```

Para establecer la dirección IP de DNS secundaria, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección_IP>
```

Configuración de los valores de DNS

- 1 **Registro del CMC.** Para registrar el CMC en el servidor DNS, escriba:

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

 **NOTA:** Algunos servidores DNS sólo registran nombres con 31 caracteres o menos. Asegúrese que el nombre designado esté dentro del límite requerido de DNS.

 **NOTA:** Los siguientes valores sólo son válidos si ha registrado el CMC en el servidor DNS estableciendo `cfgDNSRegisterRac` en 1.

- 1 **Nombre del CMC.** De manera predeterminada, el nombre de la CMC del servidor DNS es `cmc-<etiqueta de servicio>`. Para cambiar el nombre del CMC en el servidor DNS, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSRacName <nombre>
```

donde `<nombre>` es una cadena de hasta 63 caracteres alfanuméricos y guiones; el nombre debe comenzar con una letra. Por ejemplo, `cmc-1, d-345`.

- 1 **Nombre del dominio DNS.** El nombre predeterminado del dominio DNS es un solo carácter en blanco. Para establecer un nombre de dominio DNS, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSDomainName <nombre>
```

donde `<nombre>` es una cadena de hasta 254 caracteres alfanuméricos y guiones; el nombre del dominio DNS debe comenzar con una letra. Por ejemplo: `p45, a-tz-1, r-id-001`.

Configuración de la negociación automática, el modo dúplex y la velocidad de la red

Cuando está activada, la función de negociación automática determina si el CMC establece automáticamente el modo dúplex y la velocidad de la red, comunicándose con el enrutador o el conmutador más cercano. La negociación automática está activada de manera predeterminada.

Usted puede desactivar la negociación automática y especificar el modo dúplex y la velocidad de la red, escribiendo:

```
racadm config -g cfgNetTuning -o cfgNetTuningNicEnable 0
```

```
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <modo dúplex> donde:
```

- 1 `<modo dúplex>` es 0 (dúplex medio) o 1 (dúplex completo, valor predeterminado)

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <velocidad>
```

donde:

- 1 `<velocidad>` es 10 o 100 (valor predeterminado).

Establecimiento de la unidad de transmisión máxima (MTU)

La propiedad MTU le permite establecer un límite para el paquete más grande que se puede pasar a través de la interfaz. Para establecer la MTU, escriba:

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

donde `<mtu>` es un valor entre 576 y 1500 (inclusive; el valor predeterminado es 1500)

Establecimiento de la dirección IP del servidor SMTP

Usted puede activar el CMC para enviar alertas por correo electrónico con el protocolo simple de transferencia de correo (SMTP) a una dirección IP específica. Para activar esta función, escriba:

```
racadm config -g cfgRemoteHosts -o cfgRhostsFWUpdateIpAddr <dirección IP de SMTP>
```

donde `<dirección IP de SMTP>` es la dirección IP del servidor SMTP de la red.

 **NOTA:** Si la red tiene un servidor SMTP que genera y renueva arrendamientos de direcciones IP periódicamente, y las direcciones son distintas, habrá un periodo durante el que el valor de esta propiedad no funcionará debido al cambio en la dirección IP del servidor SMTP especificada. En estos casos, use el nombre DNS.

Configuración de los valores de seguridad de la red

 **NOTA:** Para realizar los siguientes pasos, debe tener privilegios de **Administrador de configuración del chasis**.

Activación de la verificación del rango de IP

El filtrado de IP compara la dirección IP?de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de `cfgRacTuning`:

```
1  cfgRacTuneIpRangeAddr
1  cfgRacTuneIpRangeMask
```

La propiedad `cfgRacTuneIpRangeMask` se aplica a las direcciones IP?entrantes y a las propiedades de `cfgRacTuneIpRangeAddr`. Si los resultados son idénticos, se permite que la petición de inicio de sesión entrante tenga acceso al iDRAC. Los inicios de sesión provenientes de direcciones IP?fuera de este rango recibirán un mensaje de error.

El inicio de sesión sólo continúa si el `cfgRacTuneIpRangeMask` es cero o la dirección IP entrante es idéntica a la dirección IP especificada por `cfgRacTuneIpRangeAddr`.

Uso de RACADM para configurar usuarios

Antes de comenzar

Puede configurar hasta 16 usuarios en la base de datos de propiedades del CMC. Antes de activar manualmente a un usuario del CMC, verifique si existe algún usuario actual. Si está configurando un nuevo CMC o ejecutó el comando `racresetcfg` de RACADM, el único usuario actual es `root` con la contraseña `calvin`. El subcomando `racresetcfg` restablece al CMC a sus valores predeterminados originales.

 **AVISO:** Tenga precaución cuando utilice el comando `racresetcfg` ya que restablecerá *todos* los parámetros de configuración originales. Todos los cambios anteriores se perderán.

 **NOTA:** Los usuarios se pueden activar y desactivar con el tiempo y la desactivación de un usuario no lo borra de la base de datos. Si un usuario se desactiva y se agrega de nuevo, el usuario puede tener un número de índice distinto en cada chasis.

Para verificar si un usuario existe, abra una consola de texto de Telnet/SSH en el CMC, inicie sesión, y escriba:

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

O bien:

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

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

 **NOTA:** También puede escribir `racadm getconfig -f <myfile.cfg>` para ver o editar el archivo `myfile.cfg`, que incluye todos los parámetros de configuración del CMC.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

Si el objeto `cfgUserAdminUserName` no tiene un valor, el número de índice que indica el objeto `cfgUserAdminIndex` está disponible para su uso. Si hay un nombre después del signo "=", el nombre de usuario tomará ese índice.

 **NOTA:** Cuando activa o desactiva un usuario manualmente con el subcomando `config` de RACADM, *debe* especificar el índice con la opción `-i`. Note que el objeto `cfgUserAdminIndex` que se muestra en el ejemplo anterior contiene un carácter `#`. Asimismo, si utiliza el comando `racadm config -f racadm.cfg` para especificar el número de grupos/objetos a escribir, el índice no se podrá especificar. Se agrega un nuevo usuario al primer índice disponible. Este comportamiento brinda más flexibilidad al configurar un segundo CMC con los mismos valores que los del CMC principal.

Cómo agregar un usuario del CMC

Para agregar un nuevo usuario a la configuración del CMC, se pueden usar unos cuantos comandos básicos. Realice los procedimientos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.

3. Establezca los privilegios de usuario. Para obtener información sobre privilegios de usuario, consulte [tabla 5-9](#), [tabla 5-10](#) y tabla B-1.
4. Active el usuario.

Ejemplo

El siguiente ejemplo describe cómo agregar un nuevo usuario denominado "Juan" con la contraseña "123456" y privilegios de inicio de sesión en el CMC.

 **NOTA:** Consulte la [tabla B-1](#) para ver una lista de los valores válidos de máscara de bits para los privilegios de usuario específicos. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios habilitados.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Para verificar que el usuario se haya añadido satisfactoriamente con los privilegios correctos, use uno de los siguientes comandos:

```
racadm getconfig -u juan
```

O bien:

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

Activación de un usuario del CMC con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones), primero localice un índice de usuario disponible, realizando los pasos descritos en [Antes de comenzar](#). Luego escriba las siguientes líneas de comando con el nuevo nombre de usuario y contraseña:

 **NOTA:** Consulte la [tabla B-1](#) para ver una lista de los valores válidos de máscara de bits para los privilegios de usuario específicos. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios habilitados.

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

Desactivación de un usuario del CMC

Por medio de RACADM, sólo es posible desactivar usuarios del CMC manualmente y de forma individual. No es posible eliminar usuarios utilizando un archivo de configuración.

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

```
racadm config -g cfgUserAdmin -i 2 cfgUserAdminPrivilege 0x0
```

Configuración de alertas por correo electrónico y de SNMP

Usted puede configurar el CMC para enviar capturas de sucesos de SNMP y/o de correo electrónico cuando ocurren ciertos sucesos en el chasis. Para obtener más información e instrucciones, consulte [Cómo configurar alertas SNMP](#) y [Configuración de alertas por correo electrónico](#).

Configuración de múltiples CMC en varios chasis

Por medio de RACADM, usted puede configurar uno o CMC con propiedades idénticas.

Cuando realiza una consulta en una tarjeta de CMC específica con las identificaciones de grupo y de objeto de la tarjeta, RACADM crea el archivo de configuración `racadm.cfg` a partir de la información obtenida. Mediante la exportación del archivo a uno o varios CMC, usted puede configurar los controladores con propiedades idénticas en una cantidad de tiempo mínima.

 **NOTA:** Algunos archivos de configuración contienen información exclusiva del CMC (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros CMC.

1. Use RACADM para hacer una consulta en el CMC de destino que contiene la configuración deseada.

 **NOTA:** El archivo de configuración generado es `miarchivo.cfg`. Usted pueden cambiar el nombre del archivo.

 **NOTA:** El archivo .cfg no contiene contraseñas de usuario. Cuando el archivo .cfg se carga en el nuevo CMC, es necesario volver a agregar todas las contraseñas.

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getconfig -f miarchivo.cfg
```

 **NOTA:** El redireccionamiento de la configuración del CMC hacia un archivo por medio de `getconfig -f` sólo se admite con la interfaz de RACADM remoto.

2. Modifique el archivo de configuración usando un editor de textos simple (opcional). Cualquier formateo especial del archivo de configuración podría dañar la base de datos de RACADM.

3. Use el archivo de configuración recién creado para modificar un CMC de destino.

En el indicador de comandos, escriba:

```
racadm config -f myfile.cfg
```

4. Restablezca el CMC de destino que fue configurado. En el indicador de comandos, escriba:

```
racadm reset
```

El subcomando `getconfig -f mi_archivo.cfg` (paso 1) solicita la configuración del CMC para el CMC principal y genera el archivo `mi_archivo.cfg`. Si es necesario, usted puede cambiar el nombre del archivo o guardarlo en una ubicación diferente.

Puede usar el comando `getconfig` para realizar las siguientes acciones:

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 de usuario por nombre de usuario

El subcomando `config` carga la información en otros CMC. Server Administrator usa el comando `config` para sincronizar las bases de datos de usuarios y de contraseñas.

Creación de un archivo de configuración del CMC

El archivo de configuración del CMC, `<nombre_de_archivo>.cfg`, se usa con el comando `racadm config -f <nombre_de_archivo>.cfg` para crear un archivo de texto simple. El comando le permite generar un archivo de configuración (similar a un archivo .ini) y configurar el CMC 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).

 **NOTA:** Para obtener más información acerca del subcomando `getconfig`, consulte [getconfig](#).

RACADM analiza el archivo .cfg cuando éste se carga por primera vez en el CMC para verificar que los nombres de los grupos y los objetos presentes sean válidos y que se estén siguiendo ciertas reglas de sintaxis simples. Los errores se señalan con el número de la línea en la que se detectó el error y un mensaje explica el problema. El archivo completo se analiza para asegurar que esté correcto y se muestran todos los errores. Los comandos de escritura no se transmiten al CMC si se encuentra un error en el archivo .cfg. Usted debe corregir *todos* los errores antes de poder realizar cualquier configuración.

Para verificar si hay errores antes de crear el archivo de configuración, use la opción `-c` con el subcomando `config`. Con la opción `-c`, `config` sólo verifica la sintaxis y *no* escribe en el CMC.

Utilice las siguientes directrices al crear un archivo .cfg:

1. Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

El analizador lee en todos los índices del CMC para ese grupo. Todos los objetos dentro de ese grupo son modificaciones cuando el CMC se configura. Si un objeto modificado representa un índice nuevo, el índice se crea en el CMC durante la configuración.

1. Usted no puede especificar un índice deseado en un archivo .cfg.

Los índices se pueden crear y se pueden eliminar. Con el tiempo, el grupo se puede fragmentar con índices utilizados y no utilizados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método ofrece flexibilidad al agregar anotaciones indexadas en las que no es necesario hacer correspondencias exactas del índice entre todos los CMC que se están administrando. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo .cfg que se analiza y se ejecuta correctamente en un CMC no funcione correctamente en otro si todos los índices están llenos y se tiene que agregar un nuevo usuario.

1. Use el subcomando `racresetcfg` para configurar ambos CMC con propiedades idénticas.

Use el subcomando `racresetcfg` para restablecer el CMC a los valores predeterminados originales 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. Consulte [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#) para obtener una lista completa de objetos y grupos.

 **AVISO:** Use el subcomando `racresetcfg` para restablecer la base de datos y la configuración del NIC del CMC a los valores predeterminados originales y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas del análisis

- 1 Las líneas que comienzan con un carácter de almohadilla/numeral (#) se tratan como comentarios.

Una línea de comentario *debe* comenzar en la columna uno. Los caracteres '#' que se encuentren en cualquier otra columna se leerán como carácter #.

Algunos parámetros de módem pueden incluir caracteres # en sus cadenas. No se requiere un carácter de escape. Es posible que desee generar un archivo .cfg a partir de un comando racadm getconfig -f <nombre_de_archivo>.cfg y luego realizar un comando racadm config -f <nombre_de_archivo>.cfg para un CMC diferente, sin agregar caracteres de escape.

Ejemplo:

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<# de inicio de módem, no es un comentario>
```

- 1 Todas las anotaciones de grupos deben estar entre corchetes de apertura y de cierre ([y]).

El carácter inicial "[" que denota un nombre de grupo *debe* estar en la columna uno. Este nombre de grupo *debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en [Definiciones de grupos y objetos de bases de datos de propiedades del CMC](#).

El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto:

```
[cfgLanNetworking] -{nombre de grupo}

cfgNicIpAddress=143.154.133.121 {nombre de objeto} {valor del objeto}
```

- 1 Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor.

Se ignorarán los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de una cadena de valores se mantienen sin modificación. El carácter que se encuentre a la derecha del signo = (por ejemplo, un segundo signo = un #, [,], etc.) se tomará tal cual. Todos estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

```
[cfgLanNetworking] -{nombre de grupo}
cfgNicIpAddress=143.154.133.121 {valor del objeto}
```

- 1 El analizador de .cfg ignora una anotación de objeto de índice.

El usuario *no puede* especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva anotación en el primer índice disponible de dicho grupo.

El comando racadm getconfig -f <nombre_de_archivo>.cfg coloca un comentario frente a los objetos del índice, lo que permite ver los comentarios incluidos.

 **NOTA:** Usted puede crear un grupo indexado manualmente, con el siguiente comando:

```
racadm config -g <nombre_de_grupo> -o <objeto anclado> -i <índice 1-16> <nombre de ancla exclusivo>
```

- 1 La línea de un grupo indexado *no se puede* eliminar de un archivo .cfg. Si se elimina la línea con un editor de textos, RACADM se detendrá al analizar el archivo de configuración y le alertará del error.

El usuario debe eliminar un objeto indexado manualmente con el 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 CMC que elimine el índice del grupo especificado.

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

```
racadm getconfig -g <nombre_de_grupo> -i <índice de 1 a 16>
```

- 1 Para grupos indexados, el ancla de objeto *debe* ser el primer objeto después del par []. Los siguientes son ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]

cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
```

Si escribe racadm getconfig -f <mi_ejemplo>.cfg, el comando genera un archivo .cfg para la configuración actual del CMC. Este archivo de configuración se puede usar como ejemplo y como punto de partida para su archivo .cfg exclusivo.

Modificación de la dirección IP del CMC

Cuando modifique la dirección IP del CMC en el archivo de configuración, elimine todas las anotaciones de <variable>=<valor> innecesarias. Sólo la etiqueta variable real del grupo con [y] permanece, incluyendo las dos anotaciones <variable>=<valor> correspondientes al cambio de la dirección IP.

Ejemplo:

```
#

# Object Group "cfgLanNetworking"
```

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

Este archivo será actualizado de la siguiente manera:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

El comando `racadm config -f <mi_archivo>.cfg` analiza el archivo e identifica todos los errores por número de línea. Un archivo correcto actualizará las anotaciones adecuadas. Además, usted puede usar el mismo comando `getconfig` que se usó en el ejemplo anterior para confirmar la actualización.

Use este archivo para descargar cambios aplicables a toda la empresa o para configurar nuevos sistemas en la red con el comando `racadm getconfig -f <mi_archivo>.cfg`.

 **NOTA:** "Anchor" es una palabra reservada y no se debe usar en el archivo `.cfg`.

Solución de problemas

[Tabla 4-3](#) muestra problemas comunes relacionados con RACADM remoto.

Tabla 4-3. Uso de los comandos serie y Racadm: preguntas frecuentes

Pregunta	Respuesta
<p>Después de realizar un restablecimiento del CMC (usando el subcomando racreset de RACADM), ejecuto un comando y aparece el siguiente mensaje:</p> <pre>racadm <subcomando> Transport: ERROR: (RC=-1)</pre> <p>¿Qué significa este mensaje?</p>	<p>Debe esperar hasta que el CMC haya completado el restablecimiento antes de ejecutar otro comando.</p>
<p>Cuando uso los subcomandos de RACADM, aparecen errores que no comprendo.</p>	<p>Es posible que encuentre uno o más de los siguientes errores al utilizar RACADM:</p> <ol style="list-style-type: none"> Mensajes de errores locales: problemas como sintaxis, errores tipográficos y nombres incorrectos. <p>Ejemplo:</p> <pre>ERROR: <mensaje></pre> <p>Use el subcomando help de RACADM para mostrar la sintaxis correcta y la información de uso.</p> <ol style="list-style-type: none"> Mensajes de error relacionados con el CMC: Problemas en los que el CMC no puede realizar una acción. También podría decir "comando de racadm fallido". <p>Escriba racadm gettracelog para obtener información sobre la depuración de errores.</p>
<p>Mientras estaba utilizando RACADM remoto, la petición cambió a ">" y no puedo hacer que regrese la petición "\$".</p>	<p>Si teclaa un carácter de comillas (") en el comando, la CLI cambiará a la petición ">" y pondrá en cola todos los comandos.</p> <p>Para regresar a la petición "\$", presione <Ctrl>-d.</p>
<p>Intenté usar los siguientes comandos y recibí un error que indica "No se ha encontrado":</p> <pre>\$ logout \$ quit</pre>	<p>Los comandos para desconectar y cerrar no se admiten en la interfaz de la CLI del CMC.</p>

Actualizaciones de comandos para CMC 1.20

Los siguientes comandos fueron actualizados para la generación del CMC 1.20:

- 1 chassisaction
 - o **-d** y **-w** descartados
 - o **nongraceshutdown** agregado
- 1 gettracelog/gettracelog/getscl
 - o **-A** y **-o** no generan una salida adicional; proporcionan compatibilidad hacia atrás para secuencias existentes
- 1 getsensorinfo
 - o **-s** y **-G** descartados
- 1 serveraction
 - o **-s** es ahora **-m** para especificar un servidor
 - o **-A** aplica el comando serveraction a todos los servidores del compartimiento
 - o **graceshutdown** descartado
- 1 fwupdate
 - o agregado { **-f** **<dirección ip de servidor ftp>** **<nombre de usuario>** **<contraseña>** } para especificar una dirección IP, un nombre de usuario y una contraseña para el servidor FTP.
 - o **-c** agregado para cancelar la actualización del firmware
- 1 getpbinfo
 - o nuevos valores de informes y elementos de estado del presupuesto de alimentación agregados
- 1 getpminfo
 - o nuevo comando que proporciona elementos y valores de estado de la administración de energía

Para obtener más información sobre las actualizaciones de este comando, consulte la sección detallada sobre cada comando en [Subcomandos de RACADM](#).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Solución de problemas y recuperación

Guía del usuario

- [Información general](#)
- [Herramientas de supervisión del chasis](#)
- [Primeros pasos para solucionar problemas en un sistema remoto](#)
- [Supervisión de la alimentación y ejecución de los comandos de control de alimentación en el chasis](#)
- [Cómo ver los resúmenes del chasis](#)
- [Cómo ver la condición del chasis y de los componentes](#)
- [Cómo ver los registros de sucesos](#)
- [Uso de la consola de diagnósticos](#)
- [Interpretación de los colores y los patrones de parpadeo de los LED](#)
- [Solución de problemas de un CMC que no responde](#)
- [Solución de problemas de red](#)
- [Desactivación de una contraseña olvidada](#)
- [Solución de problemas de alertas](#)

Información general

En esta sección se explica cómo realizar tareas relacionadas con la recuperación y la solución de problemas en el sistema remoto a través de la interfaz web del CMC.

- 1 Administración de alimentación en un sistema remoto
- 1 Cómo ver la información del chasis
- 1 Cómo ver los registros de sucesos
- 1 Uso de la consola de diagnósticos
- 1 Solución de problemas de red
- 1 Solución de problemas de alertas
- 1 Desactivación de contraseña olvidada
- 1 Códigos y registros de errores

Herramientas de supervisión del chasis

Configuración de los LED para identificar componentes en el chasis

Usted puede establecer los LED de componentes para todos ellos o para componentes individuales (el chasis, los servidores y los módulos de E/S) para que parpadeen como una forma de identificar el componente en el chasis.

 **NOTA:** Para modificar estos valores, usted debe tener privilegios de **Administrador de configuración del chasis**.

Por medio de la interfaz web

Para activar el parpadeo para uno, varios o todos los LED de componentes:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Solución de problemas**.
4. Haga clic en la subficha **Identificar**. Aparecerá la página **Identificar**, donde se muestra una lista de todos los componentes en el chasis.
5. Para activar el parpadeo de un LED de componentes, marque la casilla junto al nombre del dispositivo y luego haga clic en **Parpadear**.
6. Para desactivar el parpadeo de un LED de componentes, marque la casilla junto al nombre del dispositivo y luego haga clic en **Sin parpadear**.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm setled -m <módulo> [-l <estado_del_LED>]
```

donde <módulo> especifica el módulo cuyo LED desea configurar. Opciones de configuración:

- 1 server-*n* donde *n*=1-16
- 1 switch-*n* donde *n*=1-6
- 1 cmc-active

y <estado_del_LED> especifica si el LED debe parpadear. Opciones de configuración:

- 1 0: sin parpadeo (valor predeterminado)
- 1 1: parpadeando

Cómo configurar alertas SNMP

Las capturas del protocolo simple de administración de red (SNMP), o *capturas de sucesos*, son similares a las alertas por correo electrónico. La estación de administración las usa para recibir datos no solicitados del CMC.

Usted puede configurar el CMC para generar capturas de sucesos. [Tabla 11-1](#) proporciona una descripción general de los sucesos que desencadenan alertas de SNMP y por correo electrónico. Para obtener más información sobre las alertas por correo electrónico, consulte [Configuración de alertas por correo electrónico](#).

Tabla 11-1. Sucesos del chasis que generan alertas de SNMP y por correo electrónico

Suceso	Descripción
Falla de sonda del ventilador	Un ventilador funciona demasiado lento o no funciona.
Advertencia de sonda de baterías	Una batería ha dejado de funcionar.
Advertencia de sonda de temperatura	La temperatura está llegando a un límite excesivamente alto o bajo.
Falla de sonda de temperatura	La temperatura es demasiado alta o demasiado baja para que la operación sea adecuada.
Redundancia degradada	La redundancia para los ventiladores y/o los suministros de energía se ha reducido.
Redundancia perdida	No hay redundancia restante para los ventiladores y/o los suministros de energía.
Advertencia del suministro de energía	El suministro de energía se está acercando a una condición de falla.
Falla del suministro de energía	El suministro de energía ha fallado.
Suministro de energía ausente	Un suministro de energía que se esperaba está ausente.
Falla del registro de hardware	El registro de hardware no funciona.
Advertencia del registro de hardware	El registro de hardware está casi lleno.
Servidor ausente	Un servidor esperado no está presente.
Falla del servidor	El servidor no está funcionando.
KVM ausente	Un KVM esperado no está presente.
Falla del KVM	El KVM no está funcionando.
Módulo de E/S ausente	Un módulo de E/S esperado no está presente.
Falla del módulo de E/S	El módulo de E/S no está funcionando.
Incompatibilidad de firmware	Hay una incompatibilidad de firmware para el chasis o el firmware del servidor.

Puede agregar y configurar alertas de SNMP usando la interfaz web o RACADM.

Por medio de la interfaz web

 **NOTA:** Para agregar o configurar alertas de SNMP, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Para reforzar la seguridad, Dell recomienda que cambie la contraseña predeterminada de la cuenta root (user 1). La cuenta root es la cuenta administrativa predeterminada que se incluye con la CMC. Para cambiar la contraseña predeterminada para la cuenta root, haga clic en la identificación de usuario 1 para abrir la página **Configuración de usuario**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Administración de alertas**. Aparecerá la página **Sucesos del chasis**.

4. Activar las alertas:
 - a. Seleccione las casillas de marcación de los sucesos para los que desea activar las alertas. Para activar todos los sucesos para las alertas, seleccione la casilla de marcación **Seleccionar todo**.
 - b. Haga clic en **Aplicar** para guardar la configuración.
5. Haga clic en la subficha **Configuración de capturas**. Aparecerá la página **Destino de alertas de sucesos del chasis**.
6. Escriba una dirección IP válida en un campo **Dirección IP de destino** vacío.
7. Escriba la **Cadena de comunidad de SNMP** a la que pertenece la estación de administración de destino.

 **NOTA:** La cadena de comunidad en la página **Destino de alertas de sucesos del chasis** es diferente a la cadena de comunidad en la página **Chasis→Red/Seguridad→Servicios**. La cadena de comunidad de capturas de SNMP es la comunidad que el CMC usa para capturas de salida destinadas a estaciones de administración. La cadena de comunidad en la página **Chasis→Red/Seguridad→Servicios** es la cadena de comunidad que las estaciones de administración usan para consultar el daemon (demonio) de SNMP en el CMC.

8. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Para probar cuál es el destino de las alertas de una captura de sucesos:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Administración de alertas**. Aparecerá la página **Sucesos del chasis**.
4. Haga clic en la ficha **Configuración de capturas**. Aparecerá la página **Destino de alertas de sucesos del chasis**.
5. Haga clic en **Enviar** en la columna **Probar captura**, al lado del destino.

Uso de RACADM

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.

 **NOTA:** Sólo se puede seleccionar una máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Puede ignorar el paso 2 si ya ha seleccionado una máscara de filtro.

2. Active las alertas escribiendo:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3. Especifique los sucesos para los que desea que el CMC genere alertas, escribiendo:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <valor de máscara>
```

donde *<valor de máscara>* es un valor hexadecimal entre 0x0 y 0x003ffff.

Para obtener el valor de la máscara, utilice una calculadora científica en modo hexadecimal y sume los segundos valores de las máscaras individuales (1, 2, 4, etc.) usando la tecla *<O>*.

Por ejemplo, para activar la captura de alertas para la advertencia de sonda de baterías (0x2), la falla del suministro de energía (0x1000) y la falla del KVM (0x80000), teclee 2 *<O>* 1000 *<O>* 200000 y oprima la tecla *<=>*.

El valor hexadecimal resultante es 208002 y el valor de la máscara para el comando de RACADM es 0x208002.

Tabla 11-2. Máscaras de filtro para capturas de sucesos

Suceso	Valor de la máscara de filtro
Falla de sonda del ventilador	0x1
Advertencia de sonda de baterías	0x2
Advertencia de sonda de temperatura	0x8
Falla de sonda de temperatura	0x10
Redundancia degradada	0x40
Redundancia perdida	0x80
Advertencia del suministro de energía	0x800

Falla del suministro de energía	0x1000
Suministro de energía ausente	0x2000
Falla del registro de hardware	0x4000
Advertencia del registro de hardware	0x8000
Servidor ausente	0x10000
Falla del servidor	0x20000
KVM ausente	0x40000
Falla del KVM	0x80000
Módulo de E/S ausente	0x100000
Falla del módulo de E/S	0x200000
Incompatibilidad de firmware	0x400000

4. Active las alertas de capturas, escribiendo:

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <índice>
```

donde <índice> es un valor entre 1 y 4. El CMC usa el número de índice para distinguir hasta cuatro destinos IP configurables para alertas de capturas.

5. Especifique una dirección IP de destino para recibir la alerta de capturas, escribiendo:

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <dirección IP> -i <índice>
```

donde <dirección IP> es una dirección IP válida e <índice> es el valor del índice que se especificó en el paso 4.

6. Especifique el nombre de comunidad, escribiendo:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <nombre de comunidad> -i <índice>
```

donde <nombre de comunidad> es la comunidad SNMP a la que pertenece el chasis e <índice> es el valor del índice que se especificó en los pasos 4 y 5.

Puede configurar hasta cuatro direcciones IP de destino para recibir alertas de capturas. Para agregar más direcciones IP, repita los pasos 2 a 6.

 **NOTA:** Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que especifique (1-4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgTraps -i <índice>`. Si el índice está configurado, aparecerán los valores para los objetos `cfgTrapsAlertDestIPAddr` y `cfgTrapsCommunityName`.

Para probar cuál es el destino de las alertas de una captura de sucesos:

```
racadm testtrap -i <índice>
```

donde <índice> es un valor de 1 a 4 que representa el destino de alerta que desea probar. Si no está seguro del número de índice, escriba:

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

Configuración de alertas por correo electrónico

Cuando el CMC detecta un suceso del chasis, como una advertencia del entorno o la falla de un componente, se puede configurar para enviar una alerta por correo electrónico a una o más direcciones de correo electrónico.

[Tabla 11-1](#) proporciona una descripción general de los sucesos que desencadenan alertas de SNMP y por correo electrónico. Para obtener más información sobre las alertas de SNMP, consulte [Cómo configurar alertas SNMP](#).

Puede agregar y configurar alertas de por correo electrónico a través de la interfaz web o RACADM.

Por medio de la interfaz web

 **NOTA:** Para agregar o configurar alertas de por correo electrónico, debe tener privilegios de **Administrador de configuración del chasis**.

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Administración de alertas**. Aparecerá la página **Sucesos del chasis**.
4. Activar las alertas:
 - a. Seleccione las casillas de marcación de los sucesos para los que desea activar las alertas. Para activar todos los sucesos para las alertas, seleccione la casilla de marcación **Seleccionar todo**.

- b. Haga clic en **Aplicar** para guardar la configuración.
5. Haga clic en la subficha **Configuración de la alerta por correo electrónico**. Aparecerá la página **Destinos de alertas por correo electrónico**.
 6. Especifique la dirección IP del servidor SMTP:
 - a. Ubique el campo **Servidor SMTP (correo electrónico)** y luego escriba el nombre del servidor o la dirección IP de SMTP.

 **NOTA:** Debe configurar el servidor de correo electrónico de SMTP para aceptar correos electrónicos transmitidos desde la dirección IP del CMC, una función que normalmente está desactivada en la mayoría de los servidores de correo electrónico por motivos de seguridad. Para obtener instrucciones acerca de cómo realizar esto de forma segura, consulte la documentación incluida con el servidor SMTP.

 - b. Escriba el correo electrónico originador deseado para la alerta, o deje el campo en blanco para usar el originador de correo electrónico predeterminado. El valor predeterminado es `cmc@[dirección_IP]` donde `[dirección_IP]` es la dirección IP del CMC. Si elige introducir un valor, la sintaxis del nombre del correo electrónico es `nombredecorreo@dominio`, y se puede especificar un dominio de correo electrónico de forma opcional. Si `@dominio` no se especifica y hay un dominio de red del CMC activo, la dirección de correo electrónico de `nombredecorreo@cmc.dominio` se usará como el correo electrónico de origen. Si `@dominio` no se especifica y el CMC no tiene un dominio de red activo, se usará la dirección IP del CMC (por ejemplo, `nombredecorreo@[dirección_IP]`).
 - c. Haga clic en **Aplicar** para guardar los cambios.
 7. Especifique las direcciones de correo electrónico que recibirán las alertas:
 - a. Escriba una dirección de correo electrónico válida en un campo **Dirección de correo electrónico de destino** vacío.
 - b. Escriba un **Nombre** opcional. Éste es el nombre de la entidad que recibirá el correo electrónico. Si se introduce un nombre para una dirección de correo electrónico no válida, ésta será ignorada.
 - c. Haga clic en **Aplicar** para guardar la configuración.

Para enviar un correo electrónico de prueba a un destino de alerta por correo electrónico:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Administración de alertas**. Aparecerá la página **Sucesos del chasis**.
4. Haga clic en la subficha **Configuración de la alerta por correo electrónico**. Aparecerá la página **Destinos de alertas por correo electrónico**.
5. Haga clic en **Enviar** en la columna **Dirección de correo electrónico de destino** al lado del destino.

Uso de RACADM

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.
2. Active las alertas escribiendo:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

 **NOTA:** Sólo se puede seleccionar una máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Puede ignorar el paso 3 si ya ha establecido una máscara de filtro.

3. Especifique los sucesos para los que desea que el CMC genere alertas, escribiendo:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <valor de máscara>
```

donde `<valor de máscara>` es un valor hexadecimal entre `0x0` y `0x003ffffd` y debe expresarse con los caracteres principales `0x`. [Tabla 11-2](#) proporciona máscaras de filtro para cada tipo de suceso. Para obtener instrucciones acerca de cómo calcular el valor hexadecimal para la máscara de filtro que desea activar, consulte el paso 3 en [Uso de RACADM](#).

4. Active las alertas por correo electrónico, escribiendo:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <indice>
```

donde `<indice>` es un valor entre 1 y 4. El CMC usa el número de índice para distinguir hasta cuatro direcciones de correo electrónico de destino configurables.

5. Especifique una dirección de correo electrónico de destino para recibir las alertas por correo electrónico, escribiendo:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <dirección de correo electrónico> -i <indice>
```

donde `<dirección de correo electrónico>` es una dirección de correo electrónico válida e `<indice>` es el valor del índice que se especificó en el paso 4.

6. Especifique el nombre de la persona que recibirá la alerta por correo electrónico, escribiendo:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <nombre de correo electrónico> -i <índice>
```

donde <nombre de correo electrónico> es el nombre de la persona o grupo que recibirá la alerta por correo electrónico e <índice> es el valor del índice que se especificó en los pasos 4 y 5. El nombre de correo electrónico puede contener hasta 32 caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.

Puede configurar hasta cuatro direcciones de correo electrónico de destino para recibir alertas por correo electrónico. Para agregar más direcciones de correo electrónico, repita los pasos 2 a 6.

 **NOTA:** Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que especifique (1-4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgEmailAlert -i <índice>`. Si el índice está configurado, aparecerán valores para los objetos `cfgEmailAlertAddress` y `cfgEmailAlertEmailName`.

Primeros pasos para solucionar problemas en un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas en general en el DRAC 5:

1. ¿El sistema está encendido o apagado?
 2. Si el sistema operativo está encendido, ¿se encuentra en funcionamiento, bloqueado o simplemente congelado?
 3. Si está apagado, ¿se ha apagado de forma imprevista?
-

Supervisión de la alimentación y ejecución de los comandos de control de alimentación en el chasis

Puede utilizar la interfaz web o RACADM para:

- 1 Ver el estado de alimentación actual del sistema.
- 1 Ejecute un apagado ordenado por medio del sistema operativo al reiniciar, y encienda o apague el sistema.

Para obtener información acerca de la administración de la alimentación en el CMC y sobre la configuración del presupuesto de alimentación, la redundancia y el control de alimentación, consulte [Administración de la alimentación](#).

Cómo ver el estado del presupuesto de alimentación

Para obtener instrucciones acerca de cómo ver el estado de presupuesto de alimentación para el chasis, los servidores y las unidades de suministro de energía por medio de la interfaz web o RACADM, consulte [Cómo ver el estado del presupuesto de alimentación](#).

Ejecución de una operación de control de alimentación

Para obtener instrucciones acerca de cómo encender, apagar, reiniciar o realizar el ciclo de encendido en el sistema por medio de la interfaz web del CMC o RACADM, consulte [Ejecución de operaciones de control de alimentación en el chasis](#), [Ejecución de las operaciones de control de alimentación en un módulo de E/S](#) y [Ejecución de operaciones de control de alimentación en un servidor](#).

Cómo ver los resúmenes del chasis

El CMC proporciona una recopilación de las descripciones generales del chasis, los CMC principal y en espera, el iKVM, los ventiladores, los sensores de temperatura y los módulos de E/S (IOM).

Por medio de la interfaz web

Para ver resúmenes del chasis, los CMC, el iKVM y los módulos de E/S:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Resumen**. Aparecerá la página **Resumen del chasis**.

[Tabla 11-3](#), [tabla 11-4](#), [tabla 11-5](#) y [tabla 11-6](#) describen la información proporcionada.

Tabla 11-3. Resumen del chasis

N.º	Descripción
Nombre	Muestra el nombre del chasis. El nombre identifica al chasis en la red. Para obtener información sobre la configuración del nombre del chasis, consulte Edición de los nombres de ranuras .
Model	Muestra el modelo o el fabricante del chasis. Por ejemplo, PowerEdge 2900.
Etiqueta de servicio	Muestra la etiqueta de servicio del chasis. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento.
Asset Tag	Muestra la etiqueta de propiedad del chasis.
Ubicación	Muestra la ubicación del chasis.
Protección contra fallas del CMC lista	Indica (Sí , No) si el CMC en espera (si está presente) es capaz de tomar el control en caso de una condición de falla.
Estado de la alimentación del sistema	Muestra el estado de la alimentación del sistema.

Tabla 11-4. Resumen del CMC

N.º	Descripción
Información del CMC principal	
Nombre	Muestra el nombre del CMC. Por ejemplo, CMC principal o CMC en espera.
Descripción	Proporciona una breve descripción del propósito del CMC.
Fecha/Hora	Indica la fecha y la hora establecidos en el CMC activo o principal.
Ubicación	Indica la ubicación de la ranura del CMC activo o principal.
Versión del firmware principal	Indica la versión del firmware del CMC activo o principal.
Última actualización del firmware	Indica la fecha en la que se actualizó el firmware por última vez. Si no se ha realizado ninguna actualización, esta propiedad mostrará el valor N/A .

Versión del hardware	Indica la versión del hardware del CMC activo o principal.
MAC Address	Indica la dirección MAC del NIC del CMC. La dirección MAC es un identificador único del CMC en toda la red.
Dirección IP	Indica la dirección IP del NIC del CMC.
Puerta de enlace	Indica la puerta de enlace del NIC del CMC.
Máscara de subred	Indica la máscara de subred del NIC del CMC.
Usar DHCP (para la dirección IP del NIC)	Indica si el CMC está habilitado para solicitar y obtener una dirección IP automáticamente a partir del servidor de protocolo de configuración dinámica de host (DHCP) (Sí o No). El valor predeterminado para esta propiedad es No .
Servidor DNS principal	Indica el nombre del servidor DNS principal.
Servidor DNS alternativo	Indica el nombre del servidor DNS alternativo.
Usar DHCP para el nombre del dominio de DNS	Indica el uso de DHCP para adquirir el nombre del dominio DNS (Sí , No).
Nombre del dominio DNS	Indica el nombre del dominio DNS.
Información del CMC en espera	
Presente	Muestra (Sí , No) si hay un segundo CMC (en espera) instalado.
Versión del firmware en espera	Muestra la versión del firmware del CMC que está instalada en el CMC en espera.

Tabla 11-5. Resumen del iKVM

N.º	Descripción
Presente	Indica si el módulo iKVM está presente (Sí o No).
Nombre	Muestra el nombre del iKVM. El nombre identifica al iKVM en la red.

Fabricante	Muestra el modelo o el fabricante del iKVM.
Número de parte	Muestra el número de parte del iKVM. El número de parte es un identificador único que el proveedor proporciona. Las convenciones de notación de los números de parte varían de un proveedor a otro.
Versión del firmware	Indica la versión del firmware del iKVM.
Versión del hardware	Indica la versión del hardware del iKVM.
Estado de alimentación	Indica el estado de alimentación del iKVM: Encendido , Apagado N/A (ausente).
USB/vídeo del panel anterior activado	Indica si los conectores USB y VGA del panel anterior están activados (Sí o No).
Permitir acceso a la CLI del CMC desde iKVM	Indica que el acceso a la CLI está activado en el iKVM (Sí o No).

Tabla 11-6. Resumen del módulo de E/S

N.º	Descripción
Ubicación	Indica la ranura ocupada por los módulos de E/S. Las seis ranuras se identifican con un nombre de grupo (A, B o C) y un número de ranura (1 ó 2). Nombres de las ranuras: A-1, A-2, B-1, B-2, C-1 o C-2.
Presente	Indica si el módulo de E/S está presente (Sí o No).
Nombre	Muestra el nombre del módulo de E/S.
Estructura de red	Muestra el tipo de estructura de red.
Estado de alimentación	Indica el estado de la alimentación del módulo de E/S: Encendido , Apagado o N/A (Ausente).
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento.

Uso de RACADM

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.

2. Para ver los resúmenes del chasis y del CMC, escriba:

```
racadm getsysinfo
```

Para ver el resumen del iKVM, escriba:

```
racadm getkvminfo
```

Para ver el resumen del módulo de E/S, escriba:

```
racadm getioinfo
```

Cómo ver la condición del chasis y de los componentes

Por medio de la interfaz web

Para ver los resúmenes de la condición del chasis y de los componentes, escriba:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chassis (Chasis)** en el árbol del sistema. Aparecerá la página **Estado del chasis**.

La sección **Gráficos del chasis** proporciona una vista gráfica posterior y frontal del chasis. La representación gráfica proporciona una descripción visual de los componentes instalados en el chasis y su estado correspondiente.

Cada gráfico muestra una representación en tiempo real de los componentes instalados. El estado del componente está indicado por el color del gráfico secundario del componente.

- 1 Verde: el componente está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
- 1 Ámbar: el componente está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
- 1 Gris: el componente está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.

Todos los componentes muestran un cuadro de texto o una sugerencia de pantalla correspondiente cuando se ubica el cursor sobre el gráfico secundario de componentes. El estado de los componentes se actualiza en forma dinámica, y los cuadros de texto y los colores de los gráficos secundarios de los componentes se cambian automáticamente para reflejar el estado actual.

El gráfico secundario del componente también tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página de estado para ese componente.

La sección **Estado del componente** muestra el estado de cada componente con un icono. [Tabla 11-7](#) proporciona descripciones de cada icono.

Tabla 11-7. Indicadores de estado

N.º	Descripción	
	En buen estado	Indica que el componente está presente y se comunica con el CMC.
	Informativo	Muestra información sobre el componente cuando no hay cambios en su condición.
	Advertencia	Indica que sólo se han emitido alertas de advertencia y que se debe realizar una acción correctiva dentro del marco de tiempo establecido por el administrador . Si no se ejecutan las acciones correctivas dentro del plazo especificado por el administrador, se podrían producir fallas del componente, fallas de comunicación entre el componente y el CMC y fallas críticas o graves que podrían afectar la integridad del chasis.
	Grave	Indica que se ha enviado al menos una alerta de falla. Esto significa que el CMC aún se puede comunicar con el componente y que el estado de la condición que se reporta es crítico. Se debe ejecutar una acción correctiva inmediatamente . De lo contrario, es posible que el componente falle y deje de comunicarse con el CMC.
	Unknown	Aparece cuando el chasis se enciende por primera vez. Todos los componentes del chasis aparecen inicialmente como "desconocido" hasta que se encienden completamente.
	Sin valor	Indica que el componente no está en la ranura o que el CMC no se puede comunicar con el componente. NOTA: No es posible que el chasis esté ausente.

Uso de RACADM

Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getmodinfo
```

Cómo ver los registros de sucesos

Las páginas **Registro de hardware** y **registro del CMC** muestran sucesos críticos del sistema que ocurren en el sistema administrado.

Cómo ver el registro de hardware

El CMC genera un registro de sucesos de hardware que ocurren en el chasis. Puede ver el registro de hardware por medio de la interfaz web y RACADM remoto.

 **NOTA:** Para borrar el registro de hardware, debe tener privilegios de **Administrador de borrado de registros**.

 **NOTA:** Puede configurar el CMC para enviar capturas SNMP o por correo electrónico cuando ocurran sucesos específicos. Para obtener información sobre la configuración del CMC para enviar alertas, consulte [Cómo configurar alertas SNMP](#) y [Configuración de alertas por correo electrónico](#).

Ejemplos de anotaciones en el registro de hardware

```
critical System Software event: redundancy lost

Wed May 09 15:26:28 2007 normal System Software event: log cleared was asserted

Wed May 09 16:06:00 2007 warning System Software event: predictive failure was asserted

Wed May 09 15:26:31 2007 critical System Software event: log full was asserted

Wed May 09 15:47:23 2007 unknown System Software event: unknown event
```

Por medio de la interfaz web

Usted puede ver, guardar una versión en archivo de texto y borrar el registro de hardware en la interfaz web del CMC.

[Tabla 11-8](#) ofrece descripciones de la información proporcionada en la página **Registro de hardware** en la interfaz web del CMC.

Para ver el registro de hardware:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Registros**.
4. Haga clic en la subficha **Registro de hardware**. Aparecerá la página **Registro de hardware**.

Para guardar una copia del registro de hardware en la estación de administración o en la red:

Haga clic en **Guardar registro**. Se abrirá un cuadro de diálogo; seleccione una ubicación para un archivo de texto del registro.

 **NOTA:** Como el registro se guarda como archivo de texto, no aparecerán las imágenes gráficas que se usan para indicar la gravedad en la interfaz de usuario. En el archivo de texto, la gravedad se indica con las palabras En buen estado, Informativo, Desconocido, Advertencia y Grave. Las anotaciones de hora y fecha se guardan en orden ascendente. Si <INICIO DEL SISTEMA> aparece en la columna Fecha/Hora, significa que el suceso se presentó durante el apagado o el encendido de los módulos, cuando no se tenía una fecha u hora disponibles.

Para borrar el registro de hardware:

Haga clic en **Borrar registro**.

 **NOTA:** El CMC crea una nueva anotación de registro que indica que el registro se borró.

Tabla 11-8. Información del registro de hardware

N.º	Descripción	
	 En buen estado	Indica un suceso normal que no requiere acciones correctivas.

Gravedad		Informativo	Indica una anotación informativa en un suceso en el que el estado de Gravedad no ha cambiado.
		Unknown	Indica un suceso no crítico que requiere que se realicen acciones correctivas con prontitud a fin de evitar fallas del sistema.
		Advertencia	Indica un suceso crítico que requiere de acciones correctivas inmediatas para evitar fallas del sistema.
		Grave	Indica un suceso crítico que requiere acciones correctivas inmediatas para evitar fallas del sistema.
Fecha/Hora	Indica la fecha y hora exactas en la que ocurrió el suceso (por ejemplo, Mié 2 de mayo de 2007 16:26:55). Si no se muestra una fecha/hora, el suceso se produjo durante el inicio del sistema.		
Descripción	Ofrece una breve descripción, generada por el CMC, del suceso (por ejemplo, Redundancia perdida, Se insertó un servidor).		

Uso de RACADM

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.
2. Para ver el registro de hardware, escriba:

```
racadm getssel
```

Para borrar el registro de hardware, escriba:

```
racadm clrssel
```

Cómo ver el registro del CMC

El CMC genera un registro de los sucesos relacionados con el chasis.

 **NOTA:** Para borrar el registro de hardware, debe tener privilegios de **Administrador de borrado de registros**.

Por medio de la interfaz web

Usted puede ver, guardar una versión en archivo de texto y borrar el registro del CMC en la interfaz web del CMC.

Puede volver a clasificar las anotaciones de registro por origen, fecha/hora o descripción, haciendo clic en el encabezado de la columna. Si se vuelve a hacer clic en el encabezado de la columna se invertirá el orden.

[Tabla 11-9](#) muestra descripciones de la información proporcionada en la página **Registro del CMC** en la interfaz web del CMC.

Para ver el registro del CMC:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Registros**.
4. Haga clic en la subficha **Registro del CMC**. Aparecerá la página **Registro del CMC**.

Para guardar una copia del registro del CMC en la estación de administración o en la red, haga clic en **Guardar registro**. Se abrirá un cuadro de diálogo; seleccione una ubicación para un archivo de texto del registro.

Tabla 11-9. Información del registro del CMC

Comando	Resultado
Origen	Indica la interfaz (por ejemplo, el CMC) que provocó el suceso.
Fecha/Hora	Indica la fecha y hora exactas en la que ocurrió el suceso (por ejemplo, Mié 2 de mayo de 2007 16:26:55).
Descripción	Ofrece una breve descripción de la acción, por ejemplo, si fue un inicio o cierre de sesión, una falla de inicio de sesión o un borrado de los registros. Las descripciones las genera el CMC.

Uso de RACADM

1. Abra una consola de texto de Telnet/SSH en el CMC e inicie sesión.

2. Para ver el registro de hardware, escriba:

```
racadm getraclog
```

Para borrar el registro de hardware, escriba:

```
racadm clrraclog
```

Códigos de error de actualización del firmware

El registro del CMC también puede mostrar códigos de error como parte de la información del registro. La tabla a continuación contiene los códigos de error del registro del CMC para la actualización del firmware.

Tabla 11-10. Códigos de error de actualización del firmware

Clase de error	Valor de error (hexadecimal)	Valor de error (decimal)
ERR_NO_PRIVILEGE	0x1400	5120
ERR_LOC_CMC_STATE	0x1401	5121
ERR_INV_TARG_LINK	0x1402	5122
ERR_ILLEGAL_CMC_STATE	0x1403	5123
ERR_MX_NULL_PARAM	0x1404	5124
ERR_CLASS_UNSUPPORTED	0x1405	5125
ERR_INAPPROPRIATE_REQUEST	0x1406	5126
ERR_MX_BAD_PARAM	0x1407	5127
ERR_INVALID_TARGET	0x1408	5128
ERR_URL_NOT_FOUND	0x1409	5129
ERR_CANCEL_PID_KILL	0x140A	5130
ERR_REROUTE_PEER	0x140B	5131
ERR_BAD_URL	0x140C	5132
ERR_PAYLOAD_TOO_BIG	0x140D	5133
ERR_BAD_IP_CONV	0x140E	5134
ERR_BAD_HDR_PARAM	0x140F	5135
ERR_BAD_FILENAME	0x1410	5136
ERR_TARGET_NOT_READY	0x1411	5137
ERR_TFTP_GET_FAIL	0x1412	5138
ERR_WAITPID_FAIL	0x1413	5139
ERR_REBOOT_FAIL	0x1414	5140
ERR_UNSUPPORTED_PROTOCOL	0x1415	5141
BAD_FTP_PASSWORD	0x1416	5142
ERR_FORK_FAILED	0x1417	5143
ERR_MALLOC_ERROR	0x1418	5144
ERR_PEER_ABSENT	0x1419	5145
ERR_UPDATE_FAIL	0x141A	5146
ERR_UPDATE_FAIL	0x141B	5147
ERR_IMAGE_FILE_NOT_ACCESSIBLE	0x141C	5148
ERR_FCNTL_GET_FAIL	0x141D	5149
ERR_FCNTL_SET_FAIL	0x141E	5150
ERR_POLL_FAIL	0x141F	5151
ERR_SEND_FAIL	0x1420	5152
ERR_CONNECT_FAIL	0x1421	5153
ERR_SOCKET_FAIL	0x1422	5154
ERR_RESOLVE_REMOTE_IP_ADDR_FAIL	0x1423	5155
ERR_TIMEOUT	0x1424	5156
ERR_RECV_FAIL	0x1425	5157
ERR_INVENTORY_COUNT	0x1426	5158
ERR_FWUPD_INIT_CALL	0x1427	5159
ERR_FWUPD_START_UPDATE_CALL	0x1428	5160
ERR_OP_NOT_CANCELABLE	0x1429	5161

BAD_FTP_USERNAME	0x142A	5162
DEVICE_NOT_AVAILABLE	0x142B	5163

Uso de la consola de diagnósticos

La página **Consola de diagnósticos** permite a los usuarios avanzados, o a los usuarios con ayuda del personal de asistencia técnica, diagnosticar problemas relacionados con el hardware del chasis utilizando comandos de la CLI.

 **NOTA:** Para modificar esta configuración, debe tener privilegios de **Administrador de comandos de depuración de errores**.

Para acceder a la página de **Consola de diagnósticos**:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Chassis (Chasis)** en el árbol del sistema.
3. Haga clic en la ficha **Solución de problemas**.
4. Haga clic en la subficha **Diagnósticos**. Aparecerá la página **Consola de diagnósticos**.

Para ejecutar un comando CLI de diagnóstico, escriba el comando en el campo **Introducir comando de RACADM**, y luego haga clic en **Enviar** para ejecutar el comando de diagnóstico. Aparecerá una página de resultados del diagnóstico.

Para regresar a la página **Consola de diagnósticos** haga clic en **Volver a la página Consola de diagnósticos** o **Actualizar**.

La consola de diagnósticos admite los comandos enumerados en [tabla 11-11](#) así como también los comandos de RACADM.

Tabla 11-11. Comandos de diagnóstico admitidos

Comando	Resultado
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
netstat	Imprime el contenido de la tabla de enrutamiento.
ping <dirección IP>	Verifica que sea posible acceder a la <dirección IP> de destino desde el CMC con el contenido actual de la tabla de enrutamiento. Debe escribir una dirección IP de destino en el campo a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo (es posible que se requieran algunos segundos para que el registro aparezca). El comando gettracelog -i devuelve el número de registros en el registro de rastreo. El comando gettracelog -A muestra el registro de rastreo sin los números de anotaciones.  NOTA: Este comando es sólo para uso interno de Dell. NOTA: Para obtener más información acerca del comando gettracelog, consulte gettracelog .

Interpretación de los colores y los patrones de parpadeo de los LED

Los LED del chasis proporcionan información por medio de colores y parpadeo/sin parpadeo:

- 1 Los LED que se mantienen encendidos en color verde indican que el componente está encendido. Si el LED verde está parpadeando, indica un suceso crítico pero rutinario, como una carga de firmware, durante el cual la unidad no es operativa. No indica una falla.
- 1 Un LED de color ámbar parpadeando en un módulo indica una falla en ese módulo.
- 1 El usuario puede configurar los LED de color azul parpadeando y utilizarlos para la identificación (consulte [Configuración de los LED para identificar componentes en el chasis](#)).

[Tabla 11-12](#) muestra patrones comunes de los LED en el chasis.

Tabla 11-12. Colores y patrones de parpadeo de los LED

Componente	Color del LED, patrón de parpadeo	Significado
CMC	Verde, encendido permanentemente	Encendido

	Verde, parpadeando	Se está cargando firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Maestro/principal
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Azul, apagado	Esclavo/en espera
iKVM	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando firmware
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Ámbar, apagado	Sin falla
Servidor	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Azul, apagado	Sin falla
Módulo de E/S (común)	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal/maestro de apilamiento
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Azul, apagado	Sin falla/esclavo de apilamiento
Módulo de E/S (de paso)	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	No se utiliza
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Azul, apagado	Sin falla
Ventilador	Verde, encendido permanentemente	Ventilador funcionando
	Verde, parpadeando	No se utiliza
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	Tipo de ventilador no reconocido, actualice el firmware del CMC
	Ámbar, parpadeando	Falla del ventilador; tacómetro fuera de rango
	Ámbar, apagado	No se utiliza
Unidad de suministro de energía	(Ovalado) Verde, encendido permanentemente	CA en buen estado
	(Ovalado) Verde, parpadeando	No se utiliza
	(Ovalado) Verde, apagado	CA no en buen estado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeando	Falla
	Ámbar, apagado	Sin falla
	(Circular) Verde, encendido permanentemente	CC en buen estado
(Circular) Verde, apagado	CC no en buen estado	

Solución de problemas de un CMC que no responde

 **NOTA:** No es posible iniciar sesión en el CMC en espera por medio de una consola serie.

Si no puede iniciar sesión en el CMC usando cualquiera de las interfaces (la interfaz web, Telnet, RACADM remoto o conexión serie), puede verificar la funcionalidad del CMC si se observan los indicadores LED del mismo, si se obtiene información de recuperación a través del puerto serie DB-9 o si se recupera la imagen del firmware del CMC.

Observación de los LED para aislar el problema

Desde el frente del CMC como está instalado en el chasis, verá dos indicadores LED en el lado izquierdo de la tarjeta.

LED superior: el LED verde superior indica la alimentación. Si NO está encendido:

1. Verifique que haya corriente alterna presente para al menos un suministro de energía.
2. Verifique que la tarjeta del CMC esté asentada correctamente. Puede liberar/tirar de la palanca de expulsión, desmontar el CMC y reinstalarlo asegurándose que la tarjeta esté insertada completamente y que el pestillo cierre correctamente.

LED inferior: el indicador LED inferior es de varios colores. Cuando el CMC está activo y funcionando, y no hay ningún problema, el LED inferior es azul. Si es de color ámbar, se ha detectado una falla. La falla podría ser causada por cualquiera de los siguientes tres sucesos:

- 1 Una falla del núcleo. En este caso, se debe reemplazar la tarjeta del CMC.
- 1 Una falla de autoprueba. En este caso, se debe reemplazar la tarjeta del CMC.
- 1 Una imagen dañada. En este caso, es posible recuperar el CMC mediante la carga de la imagen del firmware del CMC.

 **NOTA:** Un inicio/restablecimiento normal del CMC toma un poco más de un minuto para iniciar su sistema operativo completamente y para que esté disponible para iniciar sesión. El LED azul está activado en el CMC activo. En una configuración redundante con dos CMC, sólo el LED verde superior está activado en el CMC en espera.

Obtención de la información de recuperación desde el puerto serie DB-9

Si el LED inferior es de color ámbar, la información de recuperación debe estar disponible desde el puerto serie DB-9, que se ubica en el frente del CMC.

Para obtener la información de recuperación:

1. Instale un cable de módem NULO entre el CMC y la máquina cliente.
2. Abra el emulador de terminal de su elección (como HyperTerminal o Minicom). Configuración: 8 bits, sin paridad, sin control de flujo, velocidad en baudios de 115200.

Una falla de la memoria del núcleo mostrará un mensaje de error cada 5 segundos.

3. Pulse <Intro>. Si aparece una petición de **recuperación**, hay información adicional disponible. La petición indica el número de ranura del CMC y el tipo de falla.

Para mostrar el motivo de la falla y la sintaxis de algunos comandos, escriba

```
recover
```

y luego oprima <Entrar>. Peticiones de ejemplo:

```
recover1[self test] CMC 1 self test failure
```

```
recover2[Bad FW images] CMC2 has corrupted images
```

- 1 Si la petición indica una falla de autoprueba, no hay componentes a los que se pueda dar servicio en el CMC. El CMC está dañado y debe ser devuelto a Dell.
- 1 Si la petición indica **Imágenes de FW dañadas**, siga los pasos que se indican en [Recuperación de la imagen del firmware](#) para resolver el problema.

Recuperación de la imagen del firmware

El CMC entra al modo de recuperación cuando no es posible realizar un inicio normal del sistema operativo del CMC. En el modo de recuperación, hay un pequeño subconjunto de comandos disponible que le permiten reprogramar los dispositivos de actualización mediante la carga del archivo de actualización del firmware, **firmimg.cmc**. Éste es el mismo archivo de imagen del firmware que se usa para las actualizaciones normales del firmware. El proceso de recuperación muestra su actividad actual e inicia el sistema operativo del CMC al completarse.

Cuando escribe `recover` y luego oprime <Entrar> en la petición **recuperación**, aparece el motivo de la recuperación y los subcomandos disponibles. Un ejemplo de secuencia de recuperación podría ser:

```
recover getniccfg
```

```
recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
```

```
recover ping 192.168.0.100
```

```
recover fwupdate -g -a 192.168.0.100
```

 **NOTA:** Conecte el cable de red al RJ45 del extremo izquierdo

NOTA: En el modo de recuperación, usted no puede enviar comandos ping al CMC normalmente porque no hay ningún apilamiento de red activo. El comando `recover ping <IP del servidor TFTP>` le permite enviar comandos ping al servidor TFTP para verificar la conexión de LAN. Es posible que necesite usar el comando `recover reset` después de `setniccfg` en algunos sistemas.

Solución de problemas de red

El registro de rastreo interno del CMC le permite depurar errores de la emisión de alertas y el sistema de red del CMC. Puede acceder al registro de rastreo a través de la interfaz web del CMC (consulte [Uso de la consola de diagnósticos](#)) o de RACADM (consulte [Uso de la interfaz de línea de comandos de RACADM y gettracelog](#)).

El registro de rastreo supervisa la siguiente información:

- 1 DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben del mismo.
- 1 IP: rastrea los paquetes IP que se envían y reciben.
- 1 DDNS: rastrea solicitudes y respuestas de DNS dinámico.

El registro de rastreo también puede contener códigos de error específicos del firmware del CMC que están relacionados con el firmware interno del CMC, no con el sistema operativo del sistema administrado.

NOTA: El CMC no generará un eco para un ICMP (ping) con un tamaño de paquete mayor de 1500 bytes.

Desactivación de una contraseña olvidada

PRECAUCIÓN: Muchas de las reparaciones deben realizarlas únicamente los técnicos de servicio autorizados. El usuario debe llevar a cabo únicamente las tareas de solución de problemas y las reparaciones sencillas autorizadas en la documentación del producto, o bien indicadas por el personal de servicio y asistencia en línea o telefónica. La garantía no cubre los daños ocasionados por reparaciones que Dell no haya autorizado. Lea y siga las instrucciones de seguridad entregadas con el producto.

Para realizar acciones de administración, se requiere un usuario con privilegios de Administrador. El software del CMC tiene una función de seguridad para la protección de la contraseña de la cuenta del usuario que puede desactivarse si se olvida la contraseña de la cuenta del administrador. Si se olvida la contraseña de la cuenta del administrador, se la puede recuperar a través del puente `REST_CONTRASEÑA` en la placa del CMC.

La placa del CMC tiene un conector de restablecimiento de contraseña con dos patas como se muestra en [figura 11-1](#). Si se instala un puente en el conector de restablecimiento, la cuenta y la contraseña predeterminadas del administrador se activarán y configurarán con los valores predeterminados de **nombre de usuario: root** y **contraseña: calvin**. La cuenta del administrador se restablecerá independientemente si eliminó la cuenta o se cambió la contraseña.

NOTA: Asegúrese de que módulo del CMC esté en un estado pasivo antes de comenzar.

1. Presione el pestillo de liberación del CMC en la asa y gire la asa hacia el lado opuesto del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.

NOTA: Las descargas electrostáticas (ESD) pueden causar daños a los componentes electrónicos internos del equipo. En ciertas condiciones, las descargas electrostáticas podrían acumularse en su cuerpo o en algún objeto, y luego descargarse en otro objeto, como su CMC. Para no correr el riesgo de descargas, descargue toda electricidad estática de su cuerpo antes de tocar los componentes electrónicos internos del equipo.

2. Retire el conector de puente del conector de restablecimiento de contraseña, e inserte un puente de dos patas para activar la cuenta predeterminada del administrador. Consulte [figura 11-1](#) para localizar el puente de contraseña en la placa del CMC.

Figura 11-1. Ubicación del puente de restablecimiento de contraseña

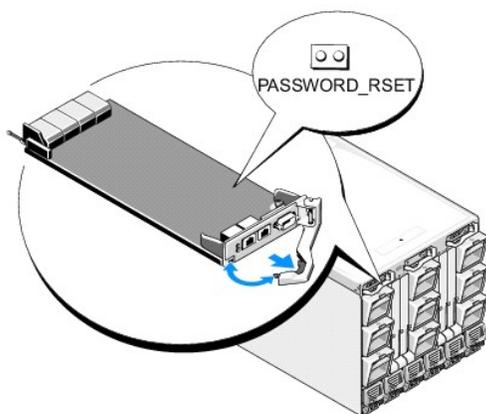


Tabla 11-13. Valores del puente de contraseña del CMC

REST_CONTRASEÑA		(Predet.)	La función de restablecimiento de contraseña está desactivada.
-----------------	--	-----------	--



La función de restablecimiento de contraseña está activada.

3. Deslice el módulo CMC hacia adentro del gabinete. Vuelva a conectar los cables que se desconectaron.
4. Inicie un cambio para hacer que el módulo activo a través de la interfaz de GUI realice los siguientes pasos:
 - a. Desplácese a la página del **chasis**, haga clic en la ficha **Administración de alimentación**, luego en la ficha **Control**.
 - b. Seleccione el botón para restablecer el **CMC (reinicio mediante sistema operativo)**.
 - c. Haga clic en **Aplicar**.
5. El CMC realiza una conmutación por error automática al módulo redundante y ese módulo se vuelve activo. Inicie sesión en el CMC activo a través del nombre de usuario de **root** y la contraseña de **calvin** predeterminados del administrador, y restaure los valores de cuenta de usuario necesarios. Las cuentas y contraseñas existentes permanecen activadas.

Después de haber completado cualquier actualización de cuenta, retire el puente de dos patas y reemplace el conector de puente.

 **NOTA:** Asegúrese de que módulo del CMC esté en un estado pasivo antes de comenzar.

1. Presione el pestillo de liberación del CMC en la asa y gire la asa hacia el lado opuesto del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.
2. Retire el puente de dos patas y reemplace el conector de puente.
3. Deslice el módulo CMC hacia adentro del gabinete. Vuelva a conectar los cables que se desconectaron.

Solución de problemas de alertas

Use el registro del CMC y el registro de rastreo para solucionar problemas de las alertas del CMC. El éxito o fracaso de cada intento de entrega de las capturas de SNMP o de correo electrónico se registra en el registro del CMC. En el registro de rastreo se incluye información adicional que describe el error particular. 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.

Puede configurar las alertas de SNMP por medio de la interfaz web. Para obtener más información, consulte [Cómo configurar alertas SNMP](#).

[Regresar a la página de contenido](#)

[Regresar a la página de contenido](#)

Uso de la interfaz web del CMC

Guía del usuario

- [Acceso a la interfaz web del CMC](#)
- [Configuración de los valores básicos del CMC](#)
- [Supervisión de la condición del sistema](#)
- [Cómo ver las identificaciones World Wide Name/Media Access Control \(WWN/MAC\)](#)
- [Configuración de las propiedades de red del CMC](#)
- [Cómo agregar y configurar usuarios del CMC](#)
- [Configuración y administración de los certificados de Microsoft Active Directory](#)
- [Protección de las comunicaciones del CMC con certificados SSL y digitales](#)
- [Administración de sesiones](#)
- [Configuración de servicios](#)
- [Configuración del presupuesto de alimentación](#)
- [Administración del firmware](#)
- [FlexAddress](#)
- [Preguntas más frecuentes](#)
- [Solución de problemas del CMC](#)

El CMC proporciona una interfaz web que permite configurar las propiedades y los usuarios del CMC, realizar tareas de administración remotas y solucionar problemas de un sistema remoto (administrado). Para la administración diaria del chasis, use la interfaz web del CMC. En este capítulo se proporciona información acerca de cómo realizar tareas de administración del chasis por medio de la interfaz web del CMC.

También puede realizar todas las tareas de configuración de la interfaz web con los comandos de RACADM local o las consolas de línea de comandos (consola serie, Telnnet o SSH). Para obtener más información acerca del uso RACADM local, consulte [Uso de la interfaz de línea de comandos de RACADM](#). Para obtener información acerca de cómo usar las consolas de línea de comandos, consulte [Configuración del CMC para el uso de consolas de línea de comandos](#).

 **NOTA:** Si utiliza Microsoft® Internet Explorer®, se conecta a través de un proxy, y recibe el error "La página XML no se puede mostrar", deberá desactivar el proxy para continuar.

Acceso a la interfaz web del CMC

Para acceder a la interfaz web del CMC:

1. Abra una ventana del explorador web compatible.

Para obtener más información, consulte [Exploradores de web compatibles](#).

2. Escriba el siguiente URL en el campo **Dirección** y luego oprima <Entrar>:

```
https://<dirección IP de CMC>
```

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

```
https://<dirección IP de CMC>:<número de puerto>
```

donde <dirección IP> es la dirección IP de la CMC y <número de puerto> corresponde al número de puerto HTTPS.

Se mostrará la página de conexión de la CMC.

Conexión

-  **NOTA:** Para iniciar sesión en el CMC, debe tener una cuenta del CMC con privilegios para **Iniciar sesión en el CMC**.
-  **NOTA:** El nombre de usuario predeterminado de la CMC es **root**, y la contraseña es **calvin**. La cuenta root es la cuenta administrativa predeterminada que se incluye con la CMC. Para reforzar la seguridad, Dell recomienda cambiar la contraseña predeterminada de la cuenta root durante la configuración inicial.
-  **NOTA:** La CMC no admite caracteres ASCII extendidos, como por ejemplo ß, å, é, ü u otros caracteres que se utilizan principalmente en idiomas distintos al inglés.
-  **NOTA:** No puede iniciar sesión en la interfaz web con diferentes nombres de usuarios en varias ventanas del explorador en una sola estación de trabajo.

Puede iniciar la sesión como un usuario de CMC o un usuario de Microsoft® Active Directory®.

Para iniciar sesión:

1. En el campo **Username (Nombre de usuario)**, escriba su nombre de usuario:

1 Nombre de usuario de la CMC: <nombre de usuario>

1 Nombre de usuario de Active Directory: <dominio>\<nombre de usuario>, <dominio>/<nombre de usuario> O <usuario>@<dominio>.

 **NOTA:** Este campo distingue entre mayúsculas y minúsculas.

2. En el campo **Password (Contraseña)**, escriba la contraseña de usuario de la CMC o de Active Directory.

 **NOTA:** Este campo distingue entre mayúsculas y minúsculas.

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

Desconexión

Cuando inicia sesión en la interfaz web, usted puede desconectarse en cualquier momento si hace clic en **Desconectar** en la esquina superior derecha de cualquier página.

 **NOTA:** Tenga cuidado al aplicar (guardar) todos los valores o la información que introduzca en una página. Si se desconecta o se desplaza a otra página sin aplicar los cambios, estos se perderán.

 **NOTA:** Si se cierra el explorador sin desconectarse primero, la sesión permanecerá abierta hasta que se acabe el tiempo de espera. Dell recomienda enfáticamente desconectarse adecuadamente: haga clic en el botón **Desconectar** antes de cerrar el explorador.

Configuración de los valores básicos del CMC

Cómo establecer el nombre del chasis

Puede establecer el nombre del chasis que se usa para identificar al chasis en la red. (El nombre predeterminado es "Dell Rack System"). Por ejemplo, una consulta del SNMP sobre el nombre del chasis regresará el nombre que usted configure.

Para establecer el nombre del chasis:

1. Inicie sesión en la interfaz web del CMC. Aparecerá la página **Estado del componente**.
2. Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración general del chasis**.
3. Escriba el nuevo nombre en el campo **Nombre del chasis** y luego haga clic en **Aplicar**.

Establecimiento de la fecha y la hora en el CMC

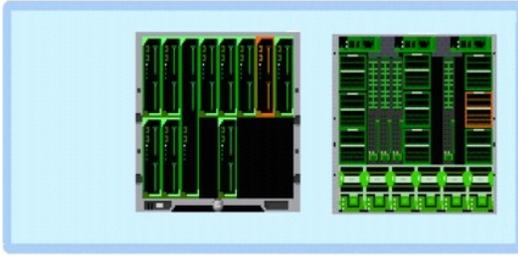
1. Inicie sesión en la interfaz web del CMC. Aparecerá la página **Estado del componente**.
2. Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración general del chasis**.
3. Haga clic en la subficha **Fecha/Hora**. Aparecerá la página **Fecha/Hora**.
4. Establezca los valores para la fecha, la hora y la zona horaria, y luego haga clic en **Aplicar**.

Supervisión de la condición del sistema

Cómo ver los resúmenes del chasis y los componentes

El CMC muestra una representación gráfica del chasis en la página **Gráficos del chasis** que proporciona una descripción visual del estado de los componentes instalados. La página **Gráficos del chasis** se actualiza en forma dinámica, y los cuadros de texto y los colores de los gráficos secundarios de los componentes se cambian automáticamente para reflejar el estado actual.

Figura 5-1. Ejemplo de gráficos de chasis en la interfaz web



La página **Estado del componente** proporciona un estado general del chasis, los CMC principales y en espera, el iKVM, las unidades de suministro de energía, los ventiladores y los módulos de E/S (IOM). La página **Resumen del chasis** proporciona un texto general del chasis, los CMC principales y en espera, el iKVM y los módulos de E/S (IOM). Para obtener instrucciones acerca de cómo ver el chasis y los resúmenes de los componentes, consulte [Cómo ver los resúmenes del chasis](#).

Cómo ver los gráficos del chasis y el estado de los componentes

La página **Gráficos del chasis** proporciona una vista gráfica posterior y frontal del chasis. La representación gráfica proporciona una descripción visual de los componentes instalados en el chasis y su estado correspondiente.

La página **Estado del componente** proporciona un estado general de todos los componentes del chasis. Para obtener instrucciones acerca de cómo ver los gráficos y el estado de los componentes, consulte [Cómo ver la condición del chasis y de los componentes](#).

Cómo ver el estado del presupuesto de alimentación

La página **Estado de presupuesto de alimentación** muestra el estado del presupuesto de alimentación del chasis, los servidores y las unidades de suministro de energía (PSU) del chasis.

Para obtener instrucciones acerca de cómo ver el estado del presupuesto de alimentación, consulte [Cómo ver el estado del presupuesto de alimentación](#). Para obtener más información acerca de la administración de la alimentación en el CMC, consulte [Administración de la alimentación](#).

Cómo ver el estado de todos los servidores

El estado de todos los servidores puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de Servidores**. **Gráficos del chasis** proporciona una descripción gráfica de todos los servidores instalados en el chasis.

Para ver el estado de todos los servidores a través de Gráficos del chasis:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección central de **Gráficos del chasis** muestra la vista frontal del chasis y contiene el estado de todos los servidores. El estado del servidor se indica mediante el color del gráfico secundario del servidor:
 - 1 Verde: el servidor está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el servidor está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el servidor está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.

La página **Estado de los servidores** proporciona descripciones generales de los servidores en el chasis.

Para ver la condición de todos los servidores:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Servidores** en el árbol del sistema. Aparece la página **Servers Status (Estado de servidores)**.

[Tabla 5-1](#) ofrece descripciones de la información proporcionada en la página **Estado de los servidores**.

Tabla 5-1. Información del estado de todos los servidores

N.º	Descripción
Nº de ranura	Muestra la ubicación del servidor. El número de ranura es un número progresivo que identifica al módulo del servidor por su ubicación dentro del chasis.
	Indica si el servidor está presente en la ranura (Sí o No). Este campo muestra la Extensión de N°

Presente	(donde el Nº será 1-8), entonces el número que lo siga será la ranura principal de un servidor con múltiples ranuras. Cuando el servidor está ausente, se desconoce (no se muestra) la información sobre la condición, el estado de la alimentación y la etiqueta de servicio del servidor.	
Estado	 En buen estado	Indica que el servidor está presente y se está comunicando con el CMC.
	 Informativo	Muestra información sobre el servidor cuando no se ha producido ningún cambio en su condición.
	 Advertencia	Indica que sólo se han generado alertas de advertencia y que se debe realizar una acción correctiva dentro del tiempo establecido por el administrador . Si las acciones correctivas no se realizan dentro del periodo especificado por el administrados, se podrían producir fallas críticas o graves que pueden afectar la integridad del dispositivo.
Condición (continuación)	 Grave	Indica que se ha emitido al menos una alerta de falla. El estado grave representa una falla del sistema en el servidor y se debe realizar una acción correctiva inmediatamente .
	Sin valor	Cuando el servidor no está presente en la ranura, no se proporciona información de su condición.
Nombre	Indica el nombre del servidor, que de manera predeterminada se identifica mediante su nombre de ranura (RANURA-01 a RANURA-16). NOTA: Puede cambiar el nombre predeterminado del servidor. Para obtener instrucciones, consulte " Edición de los nombres de ranuras ".	
Estado de la alimentación	Indica el estado de alimentación del servidor: <ul style="list-style-type: none"> o N/A: el CMC no ha determinado aún el estado de la alimentación del servidor. o Apagado: el servidor o el chasis están apagados. o Encendido: tanto el chasis como el servidor están encendidos. o Encendiendo: estado temporal entre Apagado y Encendido. Cuando la acción de finaliza satisfactoriamente, el Estado de la alimentación estará Encendido. o Apagando: estado temporal entre Encendido y Apagado. Cuando la acción de finaliza satisfactoriamente, el Estado de la alimentación estará Apagado. 	
Etiqueta de servicio	Muestra la etiqueta de servicio del servidor. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento. Si el servidor está ausente, este campo está vacío.	

Edición de los nombres de ranuras

La página **Nombres de ranuras** le permite actualizar los nombres de las ranuras en el chasis. Los nombres de las ranuras se usan para identificar a los servidores individuales. Al elegir los nombres de las ranuras se aplican las siguientes reglas:

- 1 Los nombres pueden contener **como máximo 15 caracteres ASCII imprimibles (códigos ASCII 32 al 126), salvo las comillas (", ASCII 34)**. Si se utiliza el comando de RACADM para cambiar el nombre de la ranura por medio de cualquier caracter especial, (-!@#\$\$%^&*), la cadena de nombres debe estar entre comillas para que el entorno las pase correctamente al CMC.
- 1 Los nombres de las ranuras deben ser exclusivos dentro del chasis. Dos ranuras no pueden tener el mismo nombre.
- 1 **Las cadenas no distinguen entre mayúsculas y minúsculas.** Servidor-1, servidor-1 y SERVIDOR-1 son nombres equivalentes.
- 1 Los nombres de las ranuras no deben comenzar con las siguientes cadenas:
 - 1 Commutador-
 - 1 Ventilador-
 - 1 PS-
 - 1 KVM
 - 1 DRAC-
 - 1 MC-
 - 1 Chasis
 - 1 Alojamiento-Izquierdo
 - 1 Alojamiento-Derecho
 - 1 Alojamiento-Central
- 1 Se pueden usar las cadenas Servidor-1 a Servidor-16, pero sólo para la ranura correspondiente. Por ejemplo, Servidor-3 es un nombre válido para la ranura 3, pero no para la ranura 4. Observe que Servidor-03 es un nombre válido para *cualquier* ranura.

 **NOTA:** Para cambiar un nombre de ranura en la interfaz web, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** La configuración de los nombres de ranuras en la interfaz web reside en el CMC solamente. Si un servidor se desmonta del chasis, la configuración del número de ranura no permanece con el servidor.

 **NOTA:** La configuración de los nombres de ranuras en la interfaz web del CMC siempre prevalece sobre cualquier cambio que usted aplique al nombre que aparece en la interfaz del iDRAC.

Para editar un nombre de ranura:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Servidores** en el menú **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Configuración**. Aparecerá la página **Nombres de ranuras**.
4. Escriba el nombre nuevo o actualizado de la ranura en el campo **Nombre de la ranura**. Repita esta acción para cada ranura a la que desee cambiar el nombre.
5. Haga clic en **Aplicar**.

Definición del primer dispositivo de inicio para servidores

La página **Primer dispositivo de inicio** le permite especificar el primer dispositivo de inicio del CMC para cada servidor. Es posible que éste no sea el primer dispositivo de inicio real del servidor o que represente un dispositivo presente en ese servidor; más bien, representa un dispositivo que el CMC usará como el primer dispositivo de inicio con respecto a ese servidor.

Puede definir el dispositivo de inicio predeterminado, así como un dispositivo de inicio para una sola vez, de forma que pueda iniciar una imagen especial para realizar tareas como ejecutar diagnósticos o reinstalar un sistema operativo.

El dispositivo de inicio que especifique debe existir y contener medios iniciables. [Tabla 5-2](#) muestra los dispositivos de inicio que puede especificar.

Tabla 5-2. Dispositivos de inicio

Dispositivo de inicio	Descripción
PXE	Inicio a partir de un protocolo de entorno de ejecución previo al inicio (PXE) en la tarjeta de interfaz de red.
Disco duro	Iniciar a partir del disco duro del servidor.
CD/DVD local	Inicio a partir de una unidad de CD/DVD en el servidor.
Disco flexible virtual	Inicio a partir de la unidad de disco flexible virtual. La unidad de disco flexible (o una imagen del disco flexible) está en otro equipo en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
CD/DVD virtual	Inicio a partir de una unidad de CD/DVD virtual o de una imagen ISO de CD/DVD. La unidad óptica o el archivo de imagen ISO está en otro equipo o disco disponible en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
Conexiones	Inicio a partir de un dispositivo de interfaz estándar de equipos pequeños (iSCSI) de Internet.
Tarjeta SD local	Inicie desde la tarjeta SD (Secure Digital) local: sólo para los sistemas M805/M905.
Disco flexible	Inicio a partir de un disco flexible en la unidad de disco flexible local.

 **NOTA:** Para configurar el primer dispositivo de inicio para los servidores, debe tener privilegios de **Administrador de servidores** o de **Administrador de configuración del chasis** y un nombre de usuario para iniciar sesión en el iDRAC.

Para definir el primer dispositivo de inicio para algunos o todos los servidores del chasis:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en **Servidores** en el árbol del sistema y, a continuación, haga clic en **Configuración** → **Primer dispositivo de inicio**. Se muestra una lista de servidores, uno por fila.
3. Seleccione el dispositivo de inicio que desea utilizar para cada servidor en el cuadro de lista.
4. Si desea que el servidor se inicie a partir del dispositivo seleccionado cada vez que se inicia, quite la marca de la casilla **Iniciar una vez** del servidor.
Si desea que el servidor se inicie desde el dispositivo seleccionado sólo en el siguiente ciclo de inicio, seleccione la casilla de verificación **Iniciar una vez** para el servidor.
5. Haga clic en **Aplicar**.

Cómo ver el estado de un servidor individual

El estado de un servidor individual puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de Servidores**.

La página **Gráficos del chasis** proporciona una descripción gráfica de un servidor individual instalado en el chasis.

Para ver el estado de los servidores individuales a través de Gráficos del chasis:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección central de **Gráficos del chasis** muestra la vista frontal del chasis y contiene el estado de los servidores individuales. El estado del servidor se indica mediante el color del gráfico secundario del servidor:
 - 1 Verde: el servidor está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el servidor está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el servidor está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario de un servidor individual y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre dicho servidor.
4. El gráfico secundario del servidor tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del servidor** para ese servidor.

La página **Estado del servidor** (diferente a la página **Estado de los servidores**) proporciona una descripción general del servidor y un punto de inicio a la interfaz web para el Integrated Dell Remote Access Controller (iDRAC), que es el firmware que se utiliza para administrar el servidor.

 **NOTA:** Para utilizar la interfaz para el usuario de iDRAC, usted debe tener un nombre de usuario y una contraseña de iDRAC. Para obtener más información acerca del iDRAC y del uso de la interfaz web del iDRAC, consulte la *Guía del usuario de Integrated Dell Remote Access Controller con firmware versión 1.00*.

Para ver el estado de un servidor individual:

1. Inicie sesión en la interfaz web del CMC.
2. Expanda **Servidores** en el árbol del sistema. Todos los servidores (1-16) aparecen en la lista ampliada de **Servidores**.
3. Haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.

[Tabla 5-3](#) ofrece descripciones de la información proporcionada en la página **Estado del servidor**.

Tabla 5-3. Información de estado de un servidor individual

N.º	Descripción	
Ranura	Indica la ranura ocupada por el servidor en el chasis. Los números de las ranuras son identificaciones progresivas, de 1 a 16 (hay 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis.	
Nombre de la ranura	Indica el nombre de la ranura en la que reside el servidor.	
Presente	Indica si el servidor está presente en la ranura (Presente o Ausente). Cuando el servidor está ausente, se desconoce (no se muestra) la información sobre la condición, el estado de la alimentación y la etiqueta de servicio del servidor.	
Estado		En buen estado Indica que el servidor está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del servidor.
		Informativo Muestra información acerca del servidor cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Grave).
		Advertencia Indica que sólo se han generado alertas de advertencia y que se debe realizar una acción correctiva dentro del tiempo establecido por el administrador . Si no se realizan acciones correctivas dentro del tiempo especificado por el administrador, se podrían producir fallas críticas o graves que podrían afectar la integridad del servidor.
		Grave Indica que se ha emitido al menos una alerta de falla. El estado grave representa una falla del sistema en el servidor y se debe realizar una acción correctiva inmediatamente .
	Sin valor	Cuando el servidor no está presente en la ranura, no se proporciona información de su condición.
Modelo del servidor	Indica el modelo del servidor en el chasis. Ejemplos: PowerEdge M600 o PowerEdge M605 .	
Etiqueta de servicio	Muestra la etiqueta de servicio del servidor. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento . Si el servidor está ausente, este campo está vacío.	
Firmware del iDRAC	Indica la versión del iDRAC instalada actualmente en el servidor.	
Versión del BIOS	Indica la versión del BIOS en el servidor.	
Sistema operativo	Indica el sistema operativo en el servidor.	

Cómo ver la condición de los módulos de E/S

El estado de los módulos de E/S puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de los módulos de E/S**. La página **Gráficos del chasis** proporciona una descripción gráfica de los módulos de E/S instalados en el chasis.

Para ver el estado de los módulos de E/S a través de Gráficos del chasis:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de los módulos de E/S. El estado del módulo de E/S se indica mediante el color del gráfico secundario del módulo de E/S:
 - 1 Verde: el módulo de E/S está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el módulo de E/S está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el módulo de E/S está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario individual del módulo de E/S y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre dicho módulo de E/S.
4. El gráfico secundario del módulo de E/S tiene un hipervínculo a la página correspondiente de GUI del CMC para proporcionar una exploración inmediata a la página **Estado del módulo de E/S** relacionada con dicho módulo de E/S.

La página **Estado de los módulos de E/S** proporciona descripciones generales de todos los módulos de E/S asociados con el chasis. Para obtener instrucciones acerca de cómo ver el estado de los módulos de E/S mediante la interfaz web o de la RACADM, consulte [Supervisión de la condición del módulo de E/S](#).

Cómo ver la condición de los ventiladores

 **NOTA:** Durante las actualizaciones del firmware de CMC o iDRAC en un servidor, algunos o todos los ventiladores del chasis funcionarán al 100%. Esto es normal.

El estado de todos los ventiladores puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de los ventiladores**. La página **Gráficos del chasis** proporciona una descripción gráfica de todos los ventiladores instalados en el chasis. Para ver el estado de todos los ventiladores a través de **Gráficos del chasis**:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de todos los ventiladores. El estado de los ventiladores se indica mediante el color del gráfico secundario de ventiladores:
 - 1 Verde: el ventilador está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el ventilador está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el ventilador está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario de un ventilador individual y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre ese ventilador.
4. El gráfico secundario del ventilador tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado de los ventiladores**.

La página **Estado de los ventiladores** proporciona el estado y las mediciones de velocidad (en revoluciones por minuto, o RPM) de los ventiladores en el chasis. Puede haber uno o más ventiladores.

El CMC, que controla la velocidad de los ventiladores, aumenta o disminuye automáticamente la velocidad de los mismos en función de los sucesos que se producen en todo el sistema. El CMC genera una alerta y aumenta la velocidad de los ventiladores cuando se producen los siguientes sucesos:

- 1 Se excede el umbral de temperatura ambiental del CMC.
- 1 Un ventilador falla.
- 1 Se desmonta un ventilador del chasis.

Para ver la condición de las unidades de ventilador:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Ventiladores** en el árbol del sistema. Aparecerá la página **Estado de los ventiladores**.

[Tabla 5-4](#) ofrece descripciones de la información proporcionada en la página **Estado de los ventiladores**.

Tabla 5-4. Información del estado de los ventiladores

N.º	Descripción
Presente	Indica si la unidad del ventilador está presente (Sí o No).

Estado		En buen estado	Indica que la unidad del ventilador está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y la unidad del ventilador, el CMC no puede obtener ni mostrar el estado de la condición de la unidad del ventilador.
		Grave	Indica que se ha emitido al menos una alerta de falla. Un estado grave representa una falla del sistema en la unidad del ventilador, y se debe realizar una acción correctiva inmediatamente para evitar el sobrecalentamiento y el apagado del sistema.
		Unknown	Se muestra cuando el chasis se enciende por primera vez. En caso de una falla de comunicación entre el CMC y la unidad del ventilador, el CMC no puede obtener ni mostrar el estado de la condición de la unidad del ventilador.
Nombre	Muestra el nombre del ventilador en el formato FAN-n , donde <i>n</i> es el número del ventilador.		
Velocidad	Indica la velocidad del ventilador en revoluciones por minuto (RPM).		

Cómo ver el estado del iKVM

El módulo KVM de acceso local para el chasis del servidor Dell M1000e se denomina módulo de conmutación KVM integrado Avocent®, o iKVM. El estado del iKVM asociado con el chasis puede verse en la página **Gráficos del chasis**.

Para ver el estado del iKVM a través de **Gráficos del chasis**:

1. Inicie sesión en la interfaz web del CMC.
2. Se muestra la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado del iKVM. El estado del iKVM se indica mediante el color del gráfico secundario del iKVM:
 - 1 Verde: el iKVM está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: el iKVM está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: el iKVM está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario del iKVM y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre ese iKVM.
4. El gráfico secundario del iKVM tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del iKVM**.

Para obtener instrucciones adicionales acerca de cómo ver el estado y las propiedades de configuración del iKVM, consulte:

- 1 [Cómo ver el estado y las propiedades del iKVM](#)
- 1 [Activación o desactivación del panel frontal](#)
- 1 [Activación de la consola Dell del CMC a través de iKVM](#)
- 1 [Actualización del firmware de iKVM](#)

Para obtener más información acerca de iKVM, consulte [Uso del módulo iKVM](#).

Cómo ver el estado de las unidades de suministro de energía

El estado de las unidades de suministro de energía asociadas con el chasis puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado del suministro de energía**. La página **Gráficos del chasis** proporciona una descripción gráfica de todas las unidades de suministro de energía instaladas en el chasis.

Para ver el estado de todas las unidades de suministro de energía a través de **Gráficos del chasis**:

1. Inicie sesión en la interfaz web del CMC.
2. Aparecerá la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de todas las unidades de suministro de energía. El estado de la unidad de suministro de energía se indica mediante el color del gráfico secundario de la unidad de suministro de energía:
 - 1 Verde: la unidad de suministro de energía está presente, encendida y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - 1 Ámbar: la unidad de suministro de energía está presente, pero es posible que esté encendida o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.
 - 1 Gris: la unidad de suministro de energía está presente y apagada. No se está comunicando con el CMC y no hay ninguna indicación sobre una condición adversa.
3. Use el cursor para pasar sobre un gráfico secundario de una unidad de suministro de energía individual y se mostrará un cuadro de texto o una sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre esa unidad de suministro de energía.
4. El gráfico secundario de la unidad de suministro de energía tiene un hipervínculo a la página de GUI del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del suministro de energía** para todas las unidades de suministro de energía.

La página **Estado del suministro de energía** muestra el estado y las lecturas de las unidades de suministro de energía asociadas con el chasis. Para obtener

más información acerca de la administración de la alimentación en el CMC, consulte [Administración de la alimentación](#).

Para ver la condición de las unidades de suministro de energía:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Suministros de energía** en el árbol del sistema. Aparecerá la página **Estado del suministro de energía**.

[Tabla 5-5](#) ofrece descripciones de la información proporcionada en la página **Estado del suministro de energía**.

Tabla 5-5. Información del estado del suministro de energía

N.º	Descripción	
Presente	Indica si el suministro de energía está presente (Sí o No).	
Estado	 En buen estado	Indica que la unidad de suministro de energía está presente y se está comunicando con el CMC. Indica que la unidad de suministro de energía se encuentra en buen estado. En caso de una falla de comunicación entre el CMC y la unidad de ventilador, el CMC no puede obtener ni mostrar la condición de la unidad de suministro de energía.
	 Grave	Indica que la unidad de suministro de energía tiene una falla y su condición es crítica. Se debe ejecutar una acción correctiva inmediatamente . Si no lo hace, puede provocar que el componente se apague como consecuencia de una pérdida de alimentación.
	 Unknown	Se muestra cuando el chasis se enciende por primera vez. Si se presenta una falla entre el CMC y la unidad de suministro de energía, el CMC no podrá obtener o mostrar las condiciones en las que se encuentra la unidad de suministro de energía.
Nombre	Muestra el nombre de la unidad de suministro de energía: PS-n , donde n es el número del suministro de energía.	
Estado de alimentación	Indica el estado de la alimentación de la unidad de suministro de energía: En línea , Apagado o Ranura vacía .	
Capacidad	Muestra la capacidad de alimentación en vatios.	

Cómo ver el estado de los sensores de temperatura

La página **Información de los sensores de temperatura** muestra el estado y las lecturas de las sondas de temperatura de todo el chasis (el chasis, los servidores, los módulos de E/S y el iKVM).

 **NOTA:** El valor de las sondas de temperatura no se puede editar. Cualquier cambio fuera del umbral generará una alerta que provocará que la velocidad de los ventiladores varíe. Por ejemplo, si la sonda de la temperatura ambiental del CMC excede el umbral, la velocidad de los ventiladores del chasis disminuirá.

Para ver la condición de las sondas de temperatura:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Sensores de temperatura** en el árbol del sistema. Aparecerá la página **Información de los sensores de temperatura**.

[Tabla 5-6](#) ofrece descripciones de la información proporcionada en la página **Información de los sensores de temperatura**.

Tabla 5-6. Información del estado de los sensores de temperatura

N.º	Descripción
Presente	Indica si el sensor está presente (Sí) o ausente (No) en el chasis.
Identificación de temperatura	Muestra la identificación numérica de la sonda de temperatura.
Nombre	Muestra el nombre de cada sonda de temperatura en el chasis, los servidores, los módulos de E/S y el iKVM. Ejemplos: temperatura ambiental, temperatura del servidor 1, módulo de E/S 1, temperatura del iKVM.
Lectura	Indica la temperatura actual en grados centígrados.
Umbral máximo	Indica la temperatura más alta, en grados centígrados, a la que se emite una alerta de Falla.
Umbral mínimo	Indica la temperatura más baja, en grados centígrados, a la que se emite una alerta de Falla.

Cómo ver las identificaciones World Wide Name/Media Access Control (WWN/MAC)

La [página Resumen de WWN/MAC](#) le permite ver la configuración WWN y la dirección MAC de una ranura en el chasis.

Configuración de la estructura de red

La **sección Configuración de la estructura de red** muestra el tipo de estructura de red de entrada/salida que se instala para la Estructura de red A, Estructura de red B y Estructura de red C. Una marca de selección verde indica que la estructura de red está activada para FlexAddress. La función FlexAddress se utiliza para instalar direcciones WWN/MAC de ranuras persistentes y asignadas por el chasis en varias estructuras de red y ranuras en el chasis. Esta función se activa por estructura de red y por ranura.

 **NOTA:** Consulte [Uso de FlexAddress](#) para obtener más información acerca de la función FlexAddress.

Direcciones WWN/MAC

La sección **Dirección WWN/MAC** muestra información de WWN/MAC para todos los servidores. **Ubicación** muestra la ubicación de la ranura ocupada por los módulos de entrada/salida. Las seis ranuras se identifican por una combinación del nombre de grupo (A, B o C) y el número de ranura (1 o 2): nombres de las ranuras A1, A2, B1, B2, C1 o C2. **Estructura de red** muestra el tipo de la estructura de red de E/S. **Asignadas por el servidor** muestra las direcciones WWN/MAC asignadas por el servidor integradas en el hardware del controlador. **Asignadas por el chasis** muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para la ranura particular. Una marca de selección verde en las columnas **Asignadas por el servidor** o **Asignadas por el chasis** indica el tipo de direcciones activas.

Configuración de las propiedades de red del CMC

Configuración del acceso inicial al CMC

 **NOTA:** Debe tener privilegios de **Administrador de configuración del chasis** para configurar los valores de red del CMC.

1. Inicie sesión en la interfaz web.
2. Seleccione **Chasis** en el árbol del sistema. Aparecerá la página **Estado del componente**.
3. Haga clic en la ficha **Red/Seguridad**. Aparecerá la página **Configuración de la red**.
4. Active o desactive el DHCP para el CMC seleccionando o deseleccionando la casilla **Usar DHCP (para la dirección IP del NIC del CMC)**.
5. Si desactivó el DHCP, escriba la dirección IP, la puerta de enlace y la máscara de subred.
6. Haga clic en **Aplicar cambios** en la parte inferior de la página.

Configuración de los valores de red de la LAN

 **NOTA:** Para realizar los siguientes pasos, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Los valores en la página **Configuración de la red**, como la cadena de comunidad y la dirección IP del servidor SMTP, afectan tanto al CMC como a la configuración externa del chasis.

 **NOTA:** Si tiene dos CMC (principal y en espera) en el chasis y están conectados a la red, el CMC en espera asumirá automáticamente la configuración de la red en caso que el CMC principal falle.

1. Inicie sesión en la interfaz web.
2. Haga clic en la ficha **Red/Seguridad**.
3. Configure los valores de red del CMC descritos en [tabla 5-7](#).
4. Haga clic en **Aplicar cambios**.

Para configurar un rango de IP y valores de bloqueo de IP, haga clic en el botón **Configuración avanzada** (consulte [Configuración de los valores de seguridad de la red del CMC](#)).

Para actualizar el contenido de la página **Configuración de la red**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Configuración de la red**, haga clic en **Imprimir**.

Tabla 5-7. Configuración de red

Valor	Descripción
-------	-------------

Dirección MAC del CMC	Muestra la dirección MAC del chasis, que es un identificador único del chasis en toda la red de computadoras.
Activar NIC	<p>Activa el NIC del CMC.</p> <p>Valor predeterminado: Activado. Si esta opción está seleccionada:</p> <ul style="list-style-type: none"> 1 El CMC se comunicará con la red de equipos y se podrá acceder al mismo mediante ella. 1 La interfaz web, la CLI (RACADM remoto), WSMAN, Telnet y SSH relacionados con el CMC están disponibles. <p>Si esta opción no está seleccionada:</p> <ul style="list-style-type: none"> 1 El NIC del CMC no podrá comunicarse por medio de la red. 1 La comunicación con el chasis a través del CMC no estará disponible. 1 La interfaz web, la CLI (RACADM remoto), WSMAN, Telnet y SSH relacionados con el CMC no están disponibles. 1 La interfaz web del iDRAC, la CLI local, los módulos de E/S y el iKVM siguen estando disponibles. 1 Las direcciones de red del iDRAC y el CMC se podrán obtener, en este caso, de la pantalla LCD del chasis. <p>NOTA: El acceso a los otros componentes accesibles mediante la red en el chasis no se afecta cuando la red en el chasis se desactiva (o se pierde).</p>
Usar DHCP (para la dirección IP del NIC del CMC)	<p>Habilita al CMC para solicitar y obtener automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP).</p> <p>Valor predeterminado: seleccionado (activado)</p> <p>Si esta opción está seleccionada, el CMC recupera automáticamente la configuración de IP (dirección IP, máscara y puerta de enlace) de un servidor DHCP en la red. El CMC siempre tiene asignada una dirección IP exclusiva en toda la red.</p> <p>NOTA: Cuando esta función está activada, los campos de propiedad Dirección IP, Puerta de enlace y Máscara (ubicados inmediatamente después de esta opción en la página Configuración de la red) se desactivan, y todos los valores introducidos previamente para estas propiedades se ignoran.</p> <p>Si la opción <i>no</i> está seleccionada, deberá escribir manualmente la dirección IP, la puerta de enlace y la máscara en los campos de texto que se encuentran inmediatamente después de esta opción en la página Configuración de la red.</p>
Dirección IP estática del CMC	Especifica o edita la dirección IP estática para el NIC del CMC. 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 CMC. 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 estática para el NIC del CMC. Para cambiar este valor, deseleccione la casilla de marcación Usar DHCP (para dirección IP del NIC) .
Usar DHCP para obtener direcciones de servidor DNS	<p>Obtiene las direcciones primaria y secundaria del servidor DNS a partir del servidor DHCP en vez de utilizar los valores estáticos.</p> <p>Valor predeterminado: sin seleccionar (desactivado) de manera predeterminada</p> <p>NOTA: Si Usar DHCP (para la dirección IP del NIC) está activada, active la propiedad Usar DHCP para obtener direcciones de servidor DNS.</p> <p>Si esta opción está seleccionada, el CMC recupera automáticamente la dirección IP de DNS a partir del servidor DHCP en la red.</p> <p>NOTA: Cuando esta propiedad está activada, los campos de propiedades Servidor DNS preferido estático y Servidor DNS alternativo estático (que se encuentran inmediatamente después de esta opción en la página Configuración de la red) se desactivan y todos los valores que se hayan introducido anteriormente para estas propiedades se ignoran.</p> <p>Si la opción no está seleccionada, el CMC obtendrá del servidor DNS preferido estático y del servidor DNS alternativo estático la dirección IP de DNS. Las direcciones de estos servidores se especifican en los campos de texto que están inmediatamente después en la página Configuración de la red.</p>
Servidor DNS preferido estático	Especifica la dirección IP estática del servidor DNS preferido. El servidor DNS preferido estático se implementa sólo cuando la opción Usar DHCP para obtener direcciones del servidor DNS está desactivada.
Servidor DNS alternativo estático	Especifica la dirección IP estática del servidor DNS alternativo. El servidor DNS alternativo estático se implementa sólo cuando la opción Usar DHCP para obtener direcciones del servidor DNS está desactivada. Si no tiene un servidor DNS alternativo, introduzca una dirección IP de 0.0.0.0.
Registrar el CMC en DNS	<p>Esta propiedad registra el nombre del CMC en el servidor DNS.</p> <p>Valor predeterminado: sin seleccionar (desactivado) de manera predeterminada</p> <p>NOTA: Algunos servidores DNS sólo registrarán nombres con 31 caracteres o menos. Asegúrese de que el nombre designado esté dentro del límite requerido de DNS.</p>
Nombre DNS del CMC	Muestra el nombre del CMC únicamente cuando la opción Registrar el CMC en DNS está seleccionada. El nombre predeterminado del CMC es <i>CMC_etiqueta_de_servicio</i> , donde <i>etiqueta_de_servicio</i> es el número de la etiqueta de servicio del chasis, por ejemplo: CMC-00002. El número máximo de caracteres es 63. El primer carácter debe ser una letra (a-z, A-Z), seguida de un carácter alfanumérico (a-z, A-Z, 0-9) o de un guión (-).
Usar DHCP para el nombre del dominio de DNS	<p>Utiliza el nombre de dominio DNS?predeterminado. Esta casilla de marcación sólo se activa cuando la opción Usar DHCP (para la dirección IP del NIC) está seleccionada.</p> <p>Valor predeterminado: desactivado</p>
Nombre del dominio	El nombre predeterminado del dominio DNS es un carácter en blanco. Este campo sólo se puede editar cuando la casilla de

DNS	marcación Usar DHCP para el nombre del dominio DNS está seleccionada.
Negociar automáticamente	<p>Determina si el CMC establece automáticamente el modo dúplex y la velocidad de la red por medio de la comunicación con el enrutador o conmutador más cercano (Encendido), o le permite establecer el modo dúplex y la velocidad de la red manualmente (Apagado).</p> <p>Valor predeterminado: Encendido</p> <p>Si la negociación automática está activada, el CMC se comunica automáticamente con el enrutador o conmutador más cercano.</p> <p>Si la negociación automática está desactivada, usted deberá establecer manualmente el modo dúplex y la velocidad de la red.</p>
Velocidad de red	<p>Establezca el valor de la velocidad de la red en 100 Mbps o 10 Mbps para que coincida con el entorno de la red.</p> <p>NOTA: Para que el rendimiento de la red sea efectivo, el valor de la Velocidad de la red deberá coincidir con la configuración de la red. Si asigna a la Velocidad de la red un valor menor que la velocidad de la configuración de la red, el consumo de ancho de banda aumentará y la comunicación por medio de la red se hará más lenta. Determine si la red es compatible con las velocidades de red anteriores y defina el valor según corresponda. Si la configuración de la red no coincide con ninguno de estos valores Dell recomienda que use la opción Negociación automática o que consulte al fabricante del equipo de la red.</p>
Modo dúplex	<p>Establezca el valor del modo dúplex en completo o medio para que coincida con el entorno de la red.</p> <p>Implicaciones: si Negociación automática está activado para un dispositivo pero no para el otro, el dispositivo que esté usando la negociación automática podrá determinar la velocidad de la red del otro dispositivo, pero no el modo dúplex. En este caso, el modo dúplex se predetermina a la configuración de medio dúplex durante la negociación automática. Esta incompatibilidad de la configuración de dúplex hará que la conexión de red sea lenta.</p> <p>NOTA: Los valores de la velocidad de la red y del modo dúplex no están disponibles si la negociación automática está activada.</p>
MTU	<p>Establece el tamaño de la unidad de transmisión máxima (MTU) o el paquete más grande que se puede transferir mediante la interfaz.</p> <p>Rango de configuración: de 576 a 1500.</p> <p>Valor predeterminado: 1500.</p>

Configuración de los valores de seguridad de la red del CMC

 **NOTA:** Para realizar los siguientes pasos, debe tener privilegios de **Administrador de configuración del chasis**.

1. Inicie sesión en la interfaz web.
2. Haga clic en la ficha **Red/Seguridad**. Aparecerá la página **Configuración de la red**.
3. Haga clic en el botón **Configuración avanzada**. Aparecerá la página **Seguridad de la red**.
4. Configure los valores de seguridad de la red del CMC.

[Tabla 5-8](#) describe los valores de la página **Seguridad de la red**.

Tabla 5-8. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango IP, que define un rango específico de direcciones IP que puede acceder al CMC.
Dirección del rango de IP	Determina la dirección IP de base para la verificación del rango.
Máscara de rango IP	<p>Define un rango específico de direcciones IP que pueden acceder al CMC, un proceso que se denomina verificación de rango IP.</p> <p>La verificación de rango IP permite el acceso al CMC sólo desde clientes o estaciones de administración cuyas direcciones IP están dentro del rango definido por el usuario. Los demás inicios de sesión se rechazan.</p> <p>Por ejemplo,</p> <p>Máscara de rango IP: 255.255.255.0 (11111111.11111111.11111111.00000000)</p> <p>Dirección de rango IP: 192.168.0.255 (11000000.10101000.00000000.11111111)</p> <p>El rango de dirección IP resultante es cualquier dirección que contenga 192.168.0, es decir, cualquier dirección entre 192.168.0.0 y 192.168.0.255.</p>
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo preestablecido.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección.

Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro de cual se debe producir el número de fallas de bloqueo de IP para iniciar el tiempo de penalización de bloque IP.
Tiempo de penalización de bloqueo de IP	El periodo en segundos dentro del que se rechazan los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos. NOTA: Los campos Número de fallos de bloqueo de IP, Ventana de fallos de bloqueo de IP y Tiempo de penalización de bloqueo de IP están activos sólo si la casilla Bloqueo de IP activado (el campo de propiedad que precede a estos campos) está seleccionada (activada). En ese caso, debe escribir manualmente las propiedades Número de fallos de bloqueo de IP, Ventana de fallos de bloqueo de IP y Tiempo de penalización de bloqueo de IP.

5. Haga clic en **Aplicar** para guardar la configuración.

Para actualizar el contenido de la página **Seguridad de la red**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Seguridad de la red**, haga clic en **Imprimir**.

Cómo agregar y configurar usuarios del CMC

Para administrar el sistema con el CMC y mantener la seguridad del sistema, cree usuarios exclusivos con permisos administrativos específicos (o con *autoridad basada en funciones*). Para una mayor seguridad, también puede configurar alertas que se envían por correo electrónico a usuarios específicos cuando se presente un suceso específico en el sistema.

Tipos de usuarios

Hay dos tipos de usuarios: usuarios del CMC y usuarios del iDRAC. Los usuarios del CMC también se conocen como "usuarios del chasis". Como el iDRAC reside en el servidor, los usuarios del iDRAC se conocen como "usuarios del servidor".

Los usuarios del CMC pueden ser usuarios locales o usuarios de Active Directory. Los usuarios del iDRAC también pueden ser usuarios locales o usuarios de Active Directory.

Excepto cuando un usuario del CMC tiene privilegios de Server Administrator, los privilegios otorgados a los usuarios del CMC no se transfieren automáticamente al mismo usuario en un servidor, ya que los usuarios del servidor se crean independientemente de los usuarios del CMC. En otras palabras, los usuarios de Active Directory del CMC y los usuarios de Active Directory del iDRAC residen en dos ramas diferentes en el árbol de Active Directory. Para crear un usuario del servidor local, el administrador de configuración de usuarios debe conectarse directamente al servidor. El administrador de configuración de usuarios no puede crear un usuario del servidor a partir del CMC, ni viceversa. Esta regla protege la seguridad y la integridad de los servidores.

[Tabla 5-9](#), [tabla 5-10](#) y [tabla 5-11](#) describen los privilegios de los usuarios del CMC (locales o de Active Directory), y las operaciones que un usuario del CMC puede ejecutar en el chasis y en los servidores según los privilegios que se le hayan otorgado. Por lo tanto, el término usuario o usuarios se debe interpretar como usuarios del CMC. Los usuarios del servidor se especificarán explícitamente.

Tabla 5-9. Tipos de usuarios

Privilegio	Descripción
Usuario con acceso al CMC	Los usuarios que tienen privilegios de Usuario con acceso al CMC pueden iniciar sesión en el CMC. Los usuarios que sólo tienen el privilegio de inicio de sesión pueden ver todos los datos del CMC, pero no pueden agregar ni modificar datos ni ejecutar comandos. Es posible que un usuario tenga otros privilegios sin el privilegio de inicio de sesión. Esta función es útil cuando a un usuario no se le permite iniciar sesión por un tiempo. Cuando el privilegio de inicio de sesión de ese usuario se restaura, el usuario conserva todos los demás privilegios otorgados anteriormente.
Administrador de configuración del chasis	Los usuarios que tienen privilegios de administrador de configuración del chasis pueden agregar o cambiar datos que: <ul style="list-style-type: none"> 1 Identifican el chasis, como el nombre del chasis y la ubicación del mismo 1 Están asignados específicamente al chasis, como el modo IP (estático o DHCP), la dirección IP estática, la puerta de enlace estática y la máscara de subred estática 1 Brindan servicios al chasis, como la fecha y la hora, la actualización del firmware y el restablecimiento del CMC 1 Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranuras. Aunque estas propiedades se aplican a los servidores, se trata estrictamente de propiedades del chasis que se relacionan con las ranuras y no con los servidores en sí. Por este motivo, los nombres de ranura y las prioridades de ranuras se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras. <p>Cuando un servidor se cambia a otro chasis, hereda el nombre de ranura y la prioridad asignada a la ranura que ocupe en el nuevo chasis. El nombre y la prioridad de ranura anteriores se quedarán en el chasis anterior.</p>
Administrador de configuración de usuarios	Los usuarios que tienen privilegios de administrador de configuración de usuarios pueden: <ul style="list-style-type: none"> 1 Agregar un nuevo usuario 1 Eliminar un usuario existente 1 Cambiar la contraseña de un usuario 1 Cambiar los privilegios de un usuario 1 Activar o desactivar el privilegio de inicio de sesión del usuario, pero conservar el nombre del usuario y otros privilegios en la base de datos.
	Los usuarios del CMC que tienen privilegios de administrador de borrado pueden borrar el registro de hardware y el registro del CMC.

Administrador de borrado de registros	
Administrador de control del chasis (comandos avanzados)	<p>Los usuarios del CMC con privilegios de administrador de alimentación del chasis pueden realizar todas las operaciones relacionadas con la administración de alimentación:</p> <ul style="list-style-type: none"> Controlar operaciones de alimentación del chasis, incluyendo el encendido, el apagado y el ciclo de encendido.
Server Administrator	<p>El privilegio de Server Administrator es un privilegio general que otorga al usuario del CMC todos los derechos para realizar cualquier operación en los servidores que estén presentes en el chasis.</p> <p>Cuando un usuario con privilegios de Server Administrator del CMC genera una acción que se va a realizar en un servidor, el firmware del CMC envía el comando al servidor de destino sin verificar los privilegios del usuario en el servidor. Es decir, el privilegio de Server Administrator de CMC anula la falta de privilegios de administrador en el servidor.</p> <p>Si el privilegio de Server Administrator, los usuarios que hayan sido creados en el chasis sólo pueden ejecutar un comando en un servidor cuando se cumplan todas las condiciones siguientes:</p> <ul style="list-style-type: none"> El mismo nombre de usuario existe en el servidor El mismo nombre de usuario debe tener exactamente la misma contraseña en el servidor El usuario debe tener privilegios para ejecutar el comando <p>Cuando un usuario del CMC que no tiene privilegios de Server Administrator genera una acción que se va a ejecutar en un servidor, el CMC enviará un comando al servidor de destino con el nombre de inicio de sesión y la contraseña del usuario. Si el usuario no existe en el servidor o si la contraseña no coincide, se negará al usuario la capacidad de ejecutar la acción.</p> <p>Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responderá según los privilegios que el usuario tenga en el servidor. En función de los privilegios que se tengan en el servidor, el firmware del CMC decidirá si el usuario tiene derecho de ejecutar la acción.</p> <p>A continuación se muestra una lista de los privilegios y acciones en el servidor a los que se tiene derecho con el privilegio de Server Administrator. Estos derechos se aplican únicamente cuando el usuario del chasis no tiene privilegios de Server Administrator en el chasis.</p>
Server Administrator (continuación)	<p>Administrador de configuración de servidor:</p> <ul style="list-style-type: none"> Establecer dirección IP Establecer puerta de enlace Establecer máscara de subred Establecer primer dispositivo de inicio <p>Administrador de configuración de usuarios:</p> <ul style="list-style-type: none"> Establecer contraseña raíz de iDRAC Restablecimiento de iDRAC <p>Administrador de control del servidor:</p> <ul style="list-style-type: none"> Encendido Apagado Ciclo de encendido Apagado ordenado Reinicio del servidor
Usuario de alertas de prueba	<p>Los usuarios del CMC que tienen privilegios de usuario de alertas de prueba pueden enviar mensajes de alerta de prueba.</p>
Administrador de comandos de depuración de errores	<p>Los usuarios del CMC que tienen privilegios de administrador de depuración de errores pueden ejecutar comandos de diagnóstico del sistema.</p>
Administrador de estructura de red A	<p>Los usuarios del CMC que tienen privilegios de administrador de estructura de red A pueden establecer y configurar el módulo de E/S de la estructura de red A, que reside en la ranura A1 o en la ranura A2 de las ranuras de E/S.</p>
Administrador de estructura de red B	<p>Los usuarios del CMC que tienen privilegios de administrador de estructura de red B pueden establecer y configurar el módulo de E/S de la estructura de red B, que reside en la ranura B1 o en la ranura B2 de las ranuras de E/S.</p>
Administrador de estructura de red C	<p>Los usuarios del CMC que tienen privilegios de administrador de estructura de red C pueden establecer y configurar el módulo de E/S de la estructura de red C, que reside en la ranura C1 o en la ranura C2 de las ranuras de E/S.</p>

Los grupos de usuarios del CMC proporcionan una serie de grupos de usuarios que tienen privilegios de usuarios asignados previamente. Los privilegios se muestran y describen en [tabla 5-9](#). La siguiente tabla muestra los grupos de usuarios y los privilegios de usuarios predefinidos.

 **NOTA:** Si selecciona Administrador, Usuario avanzado o Usuario invitado, y luego agrega o elimina un privilegio del conjunto predefinido, el Grupo del CMC cambia automáticamente a Personalizado.

Tabla 5-10. Privilegios del grupo del CMC

Grupo de usuarios	Privilegios otorgados
Administrador	<ul style="list-style-type: none"> Usuario con acceso al CMC Administrador de configuración del chasis Administrador de configuración de usuarios Administrador de borrado de registros Server Administrator Usuario de alertas de prueba Administrador de comandos de depuración de errores Administrador de estructura de red A Administrador de estructura de red B Administrador de estructura de red C
Usuario avanzado	<ul style="list-style-type: none"> Usuario con acceso al CMC Administrador de borrado de registros Administrador de control del chasis (comandos avanzados) Server Administrator Usuario de alertas de prueba Administrador de estructura de red A Administrador de estructura de red B Administrador de estructura de red C
Usuario invitado	Usuario con acceso al CMC
Personalizado	Selección de cualquier combinación de los siguientes permisos: <ul style="list-style-type: none"> Usuario con acceso al CMC Administrador de configuración del chasis Administrador de configuración de usuarios Administrador de borrado de registros Administrador de control del chasis (comandos avanzados) Super usuario Server Administrator Usuario de alertas de prueba Administrador de comandos de depuración de errores Administrador de estructura de red A Administrador de estructura de red B Administrador de estructura de red C
Ninguno	No se asigna ningún permiso.

Tabla 5-11. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados del CMC

Conjunto de privilegios	Permisos de administrador	Usuario avanzado Permisos	Usuario invitado Permisos
Usuario con acceso al CMC	✓	✓	✓
Administrador de configuración del chasis	✓	✗	✗
Administrador de configuración de usuarios	✓	✗	✗
Administrador de borrado de registros	✓	✓	✗
Administrador de control del chasis (comandos avanzados)	✓	✓	✗
Super usuario	✓	✗	✗
Server Administrator	✓	✓	✗
Usuario de alertas de prueba	✓	✓	✗
Administrador de comandos de depuración de errores	✓	✗	✗

Administrador de estructura de red A	✓	✓	✗
Administrador de estructura de red B	✓	✓	✗
Administrador de estructura de red C	✓	✓	✗

Cómo agregar y administrar usuarios

En las páginas **Usuarios** y **Configuración de usuarios** en la interfaz web, usted puede ver información acerca de los usuarios del CMC, agregar un nuevo usuario y cambiar la configuración de un usuario existente.

Puede configurar hasta 16 usuarios locales. Si se requieren usuarios adicionales y su compañía usa el software de servicio Microsoft® Active Directory®, puede configurar Active Directory para proporcionar acceso al CMC. La configuración de Active Directory le permitirá agregar y controlar privilegios de los usuarios del CMC para sus usuarios existentes en el software de Active Directory, además de los 16 usuarios locales. Para obtener más información, consulte [Uso del CMC con Microsoft Active Directory](#).

Los usuarios se pueden conectar mediante sesiones de la interfaz web, de Telnet serie, de SSH y de iKVM. Se puede dividir un máximo de 22 sesiones activas (interfaz web, Telnet, serie, SSH e iKVM, en cualquier combinación) entre los usuarios.

 **NOTA:** Para reforzar la seguridad, Dell recomienda que cambie la contraseña predeterminada de la cuenta root (user 1). La cuenta root es la cuenta administrativa predeterminada que se incluye con la CMC. Para cambiar la contraseña predeterminada de la cuenta root, haga clic en **User ID 1 (ID de usuario 1)** para abrir la página **User Configuration (Configuración de usuario)**. Encontrará ayuda en el enlace Help (Ayuda) situado en la parte superior derecha de la página.

Para agregar y configurar usuarios del CMC:

 **NOTA:** Para realizar los pasos siguientes, deberá contar con privilegios de **Administrador de configuración de usuarios**.

1. Inicie sesión en la interfaz web.
2. Haga clic en la ficha **Red/Seguridad** y luego haga clic en la subficha **Usuarios**. Aparecerá la página **Usuarios**, donde se muestran la **Identificación de usuario**, el nombre de usuario, los privilegios del CMC y el **estado de inicio de sesión** de cada usuario, incluso los del usuario "root". No se mostrará información de usuario de las ID de usuario disponibles para la configuración.
3. Haga clic en un número de ID de usuario disponible. Se muestra la página **User Configuration (Configuración de usuario)**.

Para actualizar el contenido de la página **Users (Usuarios)**, haga clic en **Refresh (Actualizar)**. Para imprimir el contenido de la página **Users (Usuarios)**, haga clic en **Print (Imprimir)**.

4. Seleccione la configuración general para el usuario.

[Tabla 5-12](#) describe los valores **Generales** para configurar un nombre de usuario y contraseña del CMC nuevos o existentes.

Tabla 5-12. Configuración general de usuarios

Propiedad	Descripción
Identificación de usuario	(Sólo lectura) Identifica a un usuario mediante uno de 16 números progresivos preconfigurados que la CLI utiliza para propósitos de secuencias de comandos. La identificación de usuario identifica al usuario particular al configurar al usuario mediante la herramienta CLI (RACADM). Usted no puede editar la identificación del usuario. Si va a editar información del usuario "root", este campo es estático. No se puede editar el nombre de usuario "root".
Activar el usuario	Activa o desactiva el acceso del usuario al CMC.
Nombre de usuario	Establece o muestra el nombre de usuario exclusivo del CMC asociado con el usuario. El nombre de usuario puede contener hasta 16 caracteres. Los nombres de usuario del CMC no pueden incluir caracteres de diagonales (/) ni puntos (.). NOTA: Si se cambia el nombre de usuario, el nuevo nombre no aparece en la interfaz para el usuario hasta el siguiente inicio de sesión. Cualquier usuario que inicie sesión después de aplicar el nuevo nombre de usuario también podrá ver el cambio inmediatamente.
Cambiar contraseña	Permite cambiar la contraseña existente de un usuario. Establezca la nueva contraseña en el campo Contraseña nueva . La casilla de marcación Cambiar contraseña no se podrá seleccionar si se está configurando un nuevo usuario. Usted sólo la puede seleccionar al cambiar la configuración de un usuario existente.
Contraseña	Establece una contraseña nueva para un usuario existente. Para cambiar la contraseña, también debe seleccionar la casilla Cambiar contraseña . La contraseña puede contener hasta 20 caracteres, que aparecen como puntos conforme la escribe.
Confirmar la contraseña	Verifica la contraseña que introdujo en el campo Contraseña nueva . NOTA: Los campos Contraseña nueva y Confirmar contraseña nueva sólo se pueden editar cuando usted (1) configura un nuevo

usuario; o (2) edita los valores para un usuario existente y la casilla **Cambiar contraseña** está seleccionada.

5. Asigne el usuario al grupo de usuarios de CMC. [Tabla 5-9](#) describe los privilegios de los usuarios del CMC. [Tabla 5-10](#) describe los **permisos del grupo de usuarios** para los valores de los **Privilegios de usuarios del CMC**. [Tabla 5-11](#) proporciona una comparación de los privilegios entre los administradores, los usuarios avanzados y los usuarios invitados.

Cuando seleccione un valor de privilegio de usuario en el menú desplegable CMC Group (Grupo de CMC), se visualizarán los privilegios activados (que se mostrarán como casillas de verificación marcadas en la lista) de acuerdo con la configuración predefinida para ese grupo.

Puede personalizar la configuración de privilegios para el usuario marcando o desmarcando las casillas de verificación. Una vez que haya seleccionado un grupo de CMC o bien haya efectuado selecciones de privilegios de usuario personalizadas, haga clic en **Apply Changes (Aplicar cambios)** para conservar la configuración.

6. Haga clic en **Aplicar cambios**.

Para actualizar el contenido de la página **Configuración de usuario**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Configuración de usuario**, haga clic en **Imprimir**.

Configuración y administración de los certificados de Microsoft Active Directory

 **NOTA:** Para configurar los valores de Active Directory para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Para obtener más información acerca de la configuración de Active Directory y sobre cómo configurar Active Directory con el esquema estándar o un esquema ampliado, consulte [Uso del CMC con Microsoft Active Directory](#).

Puede usar el servicio de Microsoft Active Directory para configurar el software para que proporcione acceso al CMC. El servicio de Active Directory le permite agregar y controlar los privilegios de los usuarios existentes del CMC.

Para acceder a la página **Menú principal de Active Directory**:

1. Inicie sesión en la interfaz web.
2. Haga clic en la ficha **Red/Seguridad**, y luego haga clic en la subficha **Active Directory**. Aparecerá la página **Menú principal de Active Directory**.

La [tabla 5-13](#) muestra una lista de las opciones de la página Menú principal de Active Directory.

Tabla 5-13. Opciones de la página de menú principal de Active Directory

Campo	Descripción
Configurar	Configure y administre las siguientes opciones de Active Directory para el CMC: Nombre del CMC, Nombre del dominio raíz, Nombre de dominio del CMC, Tiempo de espera de autenticación de Active Directory, Selección del esquema de Active Directory (ampliado o estándar) y Grupo de funciones.
Cargar certificado de AD	Carga un certificado firmado por una autoridad de certificados para Active Directory en el CMC. Este certificado, que se obtiene de Active Directory, brinda acceso al CMC.
Descargar certificado	Descargue un certificado de servidor de CMC en la estación de administración o en el recurso compartido de red por medio del administrador de descargas de Windows. Cuando seleccione esta opción, haga clic en Siguiente y aparecerá el cuadro de diálogo Descarga de archivo . Use este cuadro de diálogo para especificar una ubicación en la estación de administración o en la red compartida para el certificado de servidor.
Ver un certificado	Muestra el certificado de servidor firmado por una autoridad de certificados para Active Directory que se ha cargado en el CMC. NOTA: De manera predeterminada, el CMC no tiene un certificado de servidor emitido por una autoridad de certificados para Active Directory. Usted debe cargar un certificado de servidor vigente y firmado por una autoridad de certificados.

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

 **NOTA:** Para configurar los valores de Active Directory para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Antes de configurar o de usar la función de Active Directory, deberá asegurarse de que el servidor de Active Directory esté configurado para comunicarse con el CMC.

1. Asegúrese de que todos los certificados de capa de conexión segura (SSL) para los servidores de Active Directory estén firmados por la misma autoridad de certificados y de que se hayan cargado en el CMC.
2. Inicie sesión en la interfaz web y desplácese al **Menú principal de Active Directory**.
3. Seleccione **Configurar** y luego haga clic en **Siguiente**. Aparecerá la página **Configuración y administración de Active Directory**.

4. Seleccione la casilla de marcación **Habilitar Active Directory**, bajo el encabezado **Valores comunes**.

5. Escriba la información requerida en los campos restantes. Consulte el apartado [tabla 5-14](#).

Tabla 5-14. Propiedades de los valores comunes de Active Directory

Valor	Descripción
Nombre del dominio raíz	<p>Especifica el nombre de dominio que Active Directory utiliza. El nombre del dominio raíz es el nombre completo con la ruta de acceso del dominio raíz para el bosque.</p> <p>NOTA: El nombre de dominio raíz debe ser un nombre de dominio válido que siga la convención para la asignación de nombres <i>x.y</i>, donde <i>x</i> es una cadena de 1 a 256 caracteres ASCII sin espacios entre los caracteres, <i>y</i> es un tipo de dominio válido, como <i>com</i>, <i>edu</i>, <i>gov</i>, <i>int</i>, <i>mil</i>, <i>net</i> u <i>org</i>.</p> <p>Valor predeterminado: nulo (vacío)</p>
Tiempo de espera de AD	<p>El tiempo en segundos de espera para que terminen las consultas a Active Directory. El valor mínimo es igual o mayor que 15 segundos.</p> <p>Valor predeterminado: 120 segundos</p>
Especificar el servidor de AD para la búsqueda (opcional)	<p>Cuando se selecciona, activa la llamada dirigida del controlador de dominio y el catálogo global. Si activa esta opción, también deberá especificar las ubicaciones del controlador de dominio y el catálogo global en la siguiente configuración.</p> <p>NOTA: El nombre que aparece en el certificado de CA de Active Directory no se comparará con el servidor especificado de Active Directory o el servidor de catálogo global.</p>
Controlador de dominio	<p>Especifica el servidor donde está instalado el servicio Active Directory.</p> <p>Esta opción sólo es válida cuando la opción Especificar servidor de AD para la búsqueda (OPCIONAL) está activada.</p>
Catálogo global	<p>Especifica la ubicación del catálogo global en el controlador de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory.</p> <p>Esta opción sólo es válida cuando la opción Especificar servidor de AD para la búsqueda (OPCIONAL) está activada.</p>

6. Seleccione un esquema de Active Directory bajo el encabezado Selección del esquema de Active Directory. Consulte el apartado [tabla 5-15](#).

7. Si seleccionó **Esquema ampliado**, escriba la siguiente información requerida en la sección Configuración del esquema ampliado y luego vaya directamente a [étape 9](#). Si seleccionó **Esquema estándar**, vaya a [étape 8](#).

1. **Nombre del dispositivo CMC:** el nombre que identifica la tarjeta CMC de manera exclusiva en Active Directory. El nombre del CMC debe ser el mismo que el nombre común del nuevo objeto del CMC que creó en el controlador de dominio. El nombre debe ser una cadena de 1 a 256 caracteres ASCII, sin espacios entre ellos. Valor predeterminado: nulo (vacío).
1. **Nombre de dominio del CMC:** el nombre DNS (cadena) del dominio en el que reside el objeto del CMC de Active Directory (ejemplo: *cmc.com*). El nombre debe ser un nombre de dominio válido que consista en *x.y*, donde *x* es una cadena de 1 a 256 caracteres ASCII sin espacios entre ellos, *y* es un tipo de dominio válido, como *com*, *edu*, *gov*, *int*, *mil*, *net* u *org*. Valor predeterminado: nulo (vacío).

 **NOTA:** No use el nombre de NetBIOS. El nombre del dominio de CMC es el nombre completo de dominio del subdominio donde se encuentra el objeto del dispositivo del CMC.

Tabla 5-15. Opciones de esquemas de Active Directory

Valor	Descripción
Usar el esquema estándar	<p>Usa el esquema estándar con Active Directory, el cual sólo utiliza objetos de grupo de Active Directory.</p> <p>Antes de configurar el CMC para usar la opción de esquema estándar de Active Directory, primero debe configurar el software de Active Directory:</p> <ol style="list-style-type: none"> 1. En un servidor de Active Directory (controlador de dominio), abra el complemento de usuarios y equipos de Active Directory. 2. Cree un grupo o seleccione un grupo existente. El nombre del grupo y el nombre de este dominio se deben configurar en el CMC, ya sea con la interfaz web o con RACADM.
Usar el esquema ampliado	<p>Usa el esquema ampliado con Active Directory, el cual sólo utiliza objetos de Active Directory definidos por Dell.</p> <p>Antes de configurar el CMC para usar la opción de esquema ampliado de Active Directory, primero debe configurar el software de Active Directory:</p> <ol style="list-style-type: none"> 1. Amplíe el esquema de Active Directory. 2. Ampliar el complemento Usuarios y equipos de Active Directory 3. Agregue usuarios del CMC y sus privilegios en Active Directory. 4. Active SSL en cada uno de los controladores de dominio. 5. Configure las propiedades de Active Directory en el CMC utilizando ya sea la interfaz web del CMC o RACADM.

8. Si seleccionó el esquema estándar, escriba la siguiente información en la sección Configuración del esquema estándar. Si seleccionó Esquema estándar, vaya a [étape 9](#).

- 1 **Grupos de funciones:** los grupos de funciones asociados con el CMC. Para cambiar la configuración de un grupo de funciones, haga clic en el número del grupo de funciones en la lista Grupos de funciones. Aparecerá la página **Configurar grupo de funciones**.

 **NOTA:** Si hace clic en el vínculo de un grupo de funciones antes de aplicar los nuevos valores que ha introducido, perderá esos valores. Para evitar la pérdida de los nuevos valores, haga clic en **Aplicar** antes de hacer clic en el vínculo de un grupo de funciones.

- 1 **Nombre de grupo:** nombre que identifica el grupo de funciones en el Active Directory asociado con la tarjeta del CMC.
- 1 **Dominio del grupo:** dominio en el que se ubica el grupo.
- 1 **Privilegio del grupo:** nivel de privilegio para el grupo.

9. Haga clic en **Aplicar** para guardar los valores.

Para actualizar el contenido de la página **Configuración y administración de Active Directory** haga clic en **Actualizar**.

Para imprimir el contenido de la página **Configuración y administración de Active Directory**, haga clic en **Imprimir**.

Para configurar los grupos de funciones para Active Directory, haga clic en el grupo de funciones individual (1 a 5). Consulte [tabla 5-10](#) y [tabla 5-9](#).

 **NOTA:** Para guardar la configuración de la página **Configuración y administración de Active Directory**, debe hacer clic en **Aplicar** antes de avanzar a la página **Grupo de funciones personalizado**.

Carga de un certificado de Active Directory firmado por una autoridad

Desde la página **Menú principal de Active Directory**:

1. Seleccione **Cargar certificado de AD** y luego haga clic en **Siguiente**. Aparecerá la página **Carga del certificado**.
2. Escriba la ruta de acceso del archivo en el campo de texto o haga clic en **Examinar** para seleccionar el archivo.

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

3. Haga clic en **Aplicar**. Si el certificado no es válido, aparecerá un mensaje de error.

Para actualizar el contenido de la página **Cargar certificado de CA de Active Directory**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Cargar certificado de CA de Active Directory**, haga clic en **Imprimir**.

Cómo ver un certificado de Active Directory firmado por una autoridad

 **NOTA:** Si cargó el certificado de servidor de Active Directory en el CMC, asegúrese que el certificado sea válido y que no haya expirado.

Desde la página **Menú principal de Active Directory**:

1. Seleccione **Ver certificado** y luego haga clic en **Siguiente**.
2. Haga clic en el botón correspondiente de la página **Ver certificado de CA de Active Directory** para continuar.

Tabla 5-16. Información del certificado de CA de Active Directory

Campo	Descripción
Número de serie	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.
Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Para actualizar el contenido de la página **Ver certificado de CA de Active Directory** haga clic en **Actualizar**.

Para imprimir el contenido de la página **Ver certificado de CA de Active Directory**, haga clic en **Imprimir**.

Protección de las comunicaciones del CMC con certificados SSL y digitales

Este apartado proporciona información acerca de las siguientes funciones de seguridad de datos que están incorporadas en el CMC:

- 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 CMC incluye un servidor web que está configurado para usar el protocolo de seguridad SSL, que es el estándar de la industria, para transferir datos cifrados a través de la Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas y es una técnica ampliamente aceptada para ofrecer comunicación cifrada y autenticada entre los clientes y servidores a fin de evitar interceptación furtiva a la información de la 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 brinda una protección de datos de alto nivel. El CMC emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está generalmente disponible para los exploradores de Internet en Norteamérica.

El servidor web del CMC incluye un certificado digital SSL firmado automáticamente de Dell (identificación de servidor). Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del servidor web mediante el envío de una solicitud al CMC 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 (denominada CA en la interfaz web) para obtener un certificado de servidor seguro. Los certificados de servidor seguro garantizan la identidad de un sistema remoto y garantizan que otros usuarios no puedan ver o cambiar la información intercambiada con dicho sistema. Para garantizar la seguridad del CMC, se recomienda enfáticamente generar una CSR, enviarla a una autoridad de certificados y cargar el certificado que se 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 autoridad de certificados recibe la solicitud de firma de certificado, la revisa y verifica la información contenida en la solicitud. Si el solicitante cumple con los estándares de seguridad de la autoridad de certificados, esta última emite un certificado que identifica al solicitante de manera exclusiva para realizar transacciones a través de redes y en Internet.

Después de que la autoridad de certificados aprueba la solicitud de firma de certificado y le envía un certificado, usted debe cargar el certificado en el firmware del CMC. La información de la solicitud de firma de certificado almacenada en el firmware del CMC debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

 **NOTA:** Para configurar los valores de SSL para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.

 **NOTA:** Todos los certificados de servidor que se carguen deben estar vigentes (no deben haber expirado) y deben estar firmados por una autoridad de certificados.

1. Inicie sesión en la interfaz web.
2. Haga clic en la ficha **Red/Seguridad** y luego haga clic en la subficha **SSL**. Aparecerá la página **Menú principal de SSL**.

Use las opciones de la página **Menú principal de SSL** para generar una CSR para enviarla a una autoridad de certificados. La información de la solicitud de firma de certificado se almacena en el firmware del CMC.

Generación de una nueva solicitud de firma de certificado

En realizar esto con seguridad, Dell recomienda enfáticamente que usted obtenga y cargue un certificado de servidor seguro en el CMC. Los certificados del servidor seguros garantizan la identidad de un sistema remoto y que la información intercambiada con el sistema remoto no puede ser vista ni cambiada por otros. Sin un certificado de servidor seguro, el CMC es vulnerable a accesos por parte de usuarios no autorizados.

Tabla 5-17. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	<p>Seleccione esta opción y haga clic en Siguiente para abrir la página Generar una solicitud de firma de certificado (CSR), en la que puede generar una solicitud CSR de un certificado de web segura para enviarla a una autoridad de certificados.</p> <p> AVISO: Cada nueva CSR sobrescribe la CSR anterior en el CMC. Para que una autoridad de certificados acepte la solicitud de firma de certificado, la solicitud en el CMC debe coincidir con el certificado recibido de la autoridad de certificados.</p>
Cargar certificado de servidor	<p>Seleccione esta opción y haga clic en Siguiente para abrir la página Carga de certificado, en la que podrá cargar un certificado existente que la empresa posea y que utilice para controlar el acceso al CMC.</p> <p> AVISO: El CMC sólo acepta certificados codificados con X509, base 64. No acepta certificados codificados DER. Al cargar un nuevo certificado se reemplaza el certificado predeterminado que se recibió con el CMC.</p>
Ver el certificado de servidor	<p>Seleccione la opción y haga clic en el botón Siguiente para abrir la página Ver certificado del servidor en donde se puede ver el certificado actual del servidor.</p>

Para obtener un certificado de servidor seguro para el CMC, debe enviar una solicitud de firma de certificado (CSR) a la autoridad de certificados de su elección. Una CSR es una solicitud digital para obtener un certificado de servidor seguro que contiene información sobre la organización y una clave de identificación única.

Cuando se genera una CSR desde la página **Generar solicitud de firma de certificado**, se le pedirá que guarde una copia en la estación de administración o en la red compartida y la información exclusiva que se utilizó para generar la CSR se almacenará en el CMC. Esta información se usará posteriormente para autenticar el certificado de servidor que reciba de la autoridad de certificados. Después de recibir el certificado de servidor de la autoridad de certificados, debe cargarlo en el CMC.

 **NOTA:** Para que el CMC acepte el certificado de servidor emitido por la autoridad de certificados, la información de autenticación contenida en el nuevo certificado debe coincidir con la información almacenada en el CMC cuando se generó la CSR.

 **AVISO:** Cuando se genera una nueva CSR, ésta sobrescribe la CSR anterior que esté en el CMC. Si se sobrescribe una CSR pendiente antes de que la autoridad de certificados otorgue el certificado de servidor correspondiente, el CMC no aceptará el certificado de servidor porque la información que usa para autenticar el certificado se ha perdido. Tome las precauciones necesarias al generar una CSR a fin de evitar sobrescribir las CSR pendientes.

Para generar una CSR:

- Desde la página **Menú principal de SSL**, seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y luego haga clic en **Siguiente**. Aparecerá la página **Generar solicitud de firma de certificado (CSR)**.

- Escriba un valor para cada atributo de la CSR.

La [tabla 5-18](#) describe las opciones de la página **Generar solicitud de firma de certificado (CSR)**.

- Haga clic en **Generar**. Aparecerá un cuadro de diálogo **Descarga de archivo**.

- Guarde el archivo `csr.txt` en la estación de administración o en la red compartida. (También puede abrir el archivo en este momento y guardarlo después). Más adelante, enviará este archivo a una autoridad de certificados.

Tabla 5-18. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	<p>El nombre exacto que se está certificando (generalmente el nombre de dominio del servidor de web, por ejemplo, <code>www.empresa_xyz.com/</code>).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos y puntos.</p> <p>Valores no válidos: caracteres no alfanuméricos distintos a los que se indicaron anteriormente (por ejemplo, @ # \$ % & *, entre otros); caracteres que se usan principalmente en idiomas distintos al inglés, por ejemplo, ß, å, é, ü.</p>
Nombre de la organización	<p>El nombre asociado con su organización (por ejemplo: Empresa XYZ).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos, puntos y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
Unidad organizacional	<p>El nombre relacionado con la unidad organizacional, como un departamento (por ejemplo: Grupo de servidores empresariales).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos, puntos y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
Localidad	<p>La ciudad o ubicación de la organización (ejemplos: Atlanta, Hong Kong).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9) y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
Estado	<p>El estado, provincia o territorio donde se encuentra la entidad que solicita la certificación (ejemplos: Texas, Nueva Gales del Sur, Andhra Pradesh).</p>

	<p>NOTA: No utilice abreviaturas.</p> <p>Valores válidos: caracteres alfanuméricos (letras mayúsculas y minúsculas, 0-9) y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
País	El país donde se ubica la organización que solicita la certificación.
Correo electrónico	La dirección de correo electrónico de su organización. Puede escribir cualquier dirección de correo electrónico que desee tener asociada con la CSR. La dirección de correo electrónico debe ser válida y contener el signo arroba (@) (por ejemplo: nombre@empresaxyz.com).

Carga de un certificado de servidor

1. Desde la página **Menú principal de SSL**, seleccione **Cargar certificado del servidor** y luego haga clic en **Siguiente**. Aparecerá la página **Carga del certificado**.
2. Escriba la ruta de acceso del archivo en el campo de texto o haga clic en **Examinar** para seleccionar el archivo.
3. Haga clic en **Aplicar**. Si el certificado no es válido, aparecerá un mensaje de error.

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

Para actualizar el contenido de la página **Carga del certificado**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Carga del certificado**, haga clic en **Imprimir**.

Cómo ver un certificado de servidor

Desde la página **Menú principal de SSL**, seleccione **Ver certificado del servidor** y luego haga clic en **Siguiente**. Aparecerá la página **Ver certificado del servidor**.

La [tabla 5-19](#) describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

Tabla 5-19. Información de certificados

Campo	Descripción
Serie	Número de serie del certificado
Sujeto	Atributos del certificado introducidos por el sujeto
Emisor	Atributos del certificado generados por el emisor
No antes	Fecha de emisión del certificado
No después	Fecha de vencimiento del certificado

Para actualizar el contenido de la página **Ver certificado del servidor** haga clic en **Actualizar**.

Para imprimir el contenido de la página **Ver certificado del servidor**, haga clic en **Imprimir**.

Administración de sesiones

La página **Sesiones** muestra todas las instancias actuales de las conexiones al chasis y le permite terminar cualquier sesión activa.

 **NOTA:** Para terminar una sesión, usted debe tener privilegios de **Administrador de configuración del chasis**.

Para administrar sesiones:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Red/Seguridad**.
4. Haga clic en la subficha **Sesiones**. Aparecerá la página **Sesiones**.

Tabla 5-20. Propiedades de la sesiones

Propiedad	Descripción
Identificación de sesión	Muestra el número de identificación generado progresivamente para cada ocurrencia de un inicio de sesión.
Nombre de usuario	Muestra el nombre de inicio de sesión del usuario (usuario local o usuario de Active Directory). Algunos ejemplos de nombres de usuario de Active Directory son <i>nombre@dominio.com</i> , <i>dominio.com/nombre</i> , <i>dominio.com\nombre</i> .
Dirección IP	Muestra la dirección IP del usuario en formato de números separados con puntos.
Tipo de sesión	Describe el tipo de sesión: Telnet, serie, SSH, RACADM remoto, SMASH CLP, WSMAN o interfaz gráfica para el usuario.
Terminar	Le permite terminar cualquiera de las sesiones de la lista, excepto la suya. Para terminar la sesión asociada, haga clic en el icono de papelera  . Esta columna sólo aparecerá si usted tiene privilegios de Administrador de configuración del chasis .

Para terminar la sesión, haga clic en el icono de papelera en la línea que describe la sesión.

Configuración de servicios

El CMC incluye un Web Server que está configurado para utilizar el protocolo de seguridad SSL estándar de la industria para aceptar y transferir datos cifrados de y para clientes en Internet. El Web Server incluye un certificado digital SSL de Dell firmado automáticamente (identificación del servidor) y es responsable de aceptar y responder solicitudes de HTTP seguras de clientes. La interfaz web y la herramienta de CLI remota requieren este servicio para comunicarse con el CMC.

-  **NOTA:** La herramienta de CLI remota (RACADM) y la interfaz web utilizan el servidor de web. Si el servidor de web no está activo, RACADM remoto y la interfaz web no funcionarán.
-  **NOTA:** En caso de un restablecimiento del Web Server, espere al menos un minuto para que los servicios estén disponibles de nuevo. Un restablecimiento del servidor de web generalmente sucede como resultado de cualquiera de los siguientes sucesos: la configuración de la red o las propiedades de seguridad de la red se cambiaron mediante la interfaz para el usuario de web del CMC o de RACADM; la configuración del puerto de Web Server se cambió mediante la interfaz de usuario de web o de RACADM; el CMC se restableció; se cargó un nuevo certificado de servidor SSL.
-  **NOTA:** Para modificar la configuración de los servicios, debe tener privilegios de **Administrador de configuración del chasis**.

Para configurar los servicios del CMC:

1. Inicie sesión en la interfaz web del CMC.
2. Haga clic en la ficha **Red/Seguridad**.
3. Haga clic en la subficha **Servicios**. Aparecerá la página **Servicios**.
4. Configure los servicios siguientes según sea necesario:
 1. Consola serie del CMC ([Tabla 5-21](#))
 1. Servidor web ([Tabla 5-22](#))
 1. SSH ([Tabla 5-23](#))
 1. Telnet ([Tabla 5-24](#))
 1. RACADM remoto ([Tabla 5-25](#))
5. Haga clic en **Aplicar**; **actualiza todo el tiempo de espera predeterminado y los límites máximos del tiempo de espera**.

Tabla 5-21. Configuración de la consola serie del CMC

Valor	Descripción
Activado	Activa la interfaz de la consola Telnet del CMC. Valor predeterminado: sin seleccionar (desactivada)
Redirección activada	Activa la redirección de la consola serie/de texto al servidor a través del cliente Telnet desde el CMC. El CMC se conecta con el iDRAC, que se conecta internamente con el servidor. Opciones de configuración: seleccionado (activado), sin seleccionar (desactivado) Valor predeterminado: sin seleccionar (desactivado)
Tiempo de espera en inactividad	Indica el número de segundos antes de que una sesión de Telnet se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Rango de tiempo de espera: 0 o 60 hasta 10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0.

	<p>Valor predeterminado: 1800 segundos</p>
Velocidad en baudios	<p>Indica la velocidad de los datos en el puerto serie externo del CMC.</p> <p>Opciones de configuración: 9600, 19200, 28800, 38400, 57600 y 115200 bps.</p> <p>Valor predeterminado: 115200 bps</p>
Autenticación desactivada	<p>Activa la autenticación del inicio de sesión de la consola serie del CMC.</p> <p>Valor predeterminado: sin seleccionar (desactivada)</p>
Tecla Escape	<p>Permite especificar la combinación de la tecla Esc que termina la redirección de la consola serie/de texto cuando se utiliza el comando connect com2.</p> <p>Valor predeterminado: ^\</p> <p>Mantenga presionada la tecla <Ctrl> y presione la tecla de barra diagonal invertida (\)</p> <p> NOTA: El carácter de intercalación ^ representa la tecla <Ctrl>.</p> <p>Opciones de configuración:</p> <ul style="list-style-type: none"> 1 Valor decimal (ejemplo: 95) 1 Valor hexadecimal (por ejemplo: 0x12) 1 Valor octal (ejemplo: 007) 1 Valor ASCII (ejemplo: ^a) <p>Los valores ASCII se pueden representar utilizando los siguientes códigos de la tecla Esc:</p> <ul style="list-style-type: none"> 1 Esc seguido por un carácter alfabético (a-z, A-Z) 1 Esc seguido por los siguientes caracteres especiales: [] \ ^ _ 1 Longitud máxima permitida: 4
Tamaño del búfer de historial	<p>Indica el tamaño máximo del búfer del historial serie, que contiene los últimos caracteres escritos en la consola serie.</p> <p>Valor predeterminado: 8192 caracteres</p>
Comando de inicio de sesión	<p>Especifica el comando serie que se ejecuta automáticamente cuando un usuario se conecta a la interfaz de la consola serie del CMC.</p> <p>Ejemplo: connect server-1</p> <p>Valor predeterminado: [Nulo]</p>

Tabla 5-22. Configuración del servidor web

Valor	Descripción
Activado	<p>Activa los servicios de Web Server (acceso mediante RACADM remoto y la interfaz web) para el CMC.</p> <p>Valor predeterminado: seleccionado (activado)</p>
N.º máx. de sesiones	<p>Indica el número máximo de sesiones simultáneas de la interfaz web del usuario permitidas para el chasis. Un cambio en la propiedad N.º máx. de sesiones tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluyendo la suya). La propiedad N.º máx. de sesiones para el Web Server no afecta a la RACADM.</p> <p>Rango permitido: 1 a 4</p> <p>Valor predeterminado: 4</p> <p>NOTA: Si cambia la propiedad N.º máx. de sesiones a un valor menor que el número de sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.</p>
Tiempo de espera en inactividad	<p>Indica el número de segundos antes de que una sesión de interfaz web del usuario inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual.</p> <p>Rango de tiempo de espera: 60 a 10800 segundos.</p> <p>Valor predeterminado: 1800 segundos</p>
Número de puerto de HTTP	<p>Indica el puerto predeterminado utilizado por el CMC en espera de una conexión de servidor.</p> <p>NOTA: Cuando se proporciona una dirección HTTP en el explorador, el servidor de web se redirige automáticamente y utiliza HTTPS.</p> <p>Si se ha cambiado el número predeterminado del puerto HTTPS predeterminado (80), debe incluir el número de puerto en la dirección introducida en el campo de dirección del explorador, como se muestra:</p> <p style="text-align: center;">http://<dirección IP>:<número de puerto></p> <p>donde <i>dirección IP</i> es la dirección IP del chasis y <i>número de puerto</i> es el número de puerto HTTP distinto al predeterminado de 80.</p>

	<p>Rango de configuración: de 10 a 65535</p> <p>Valor predeterminado: 80</p>
Número de puerto de HTTPS	<p>Indica el puerto predeterminado utilizado por el CMC en espera de una conexión segura de servidor.</p> <p>Si el número del puerto HTTPS predeterminado (443) se ha cambiado, debe incluir el número de puerto en la dirección introducida en campo de dirección del explorador, como se muestra:</p> <p style="text-align: center;">http://<dirección IP>:<número de puerto></p> <p>donde <dirección IP> es la dirección IP del chasis y <número de puerto> es el número de puerto HTTPS distinto al valor predeterminado de 443.</p> <p>Rango de configuración: de 10 a 65535</p> <p>Valor predeterminado: 443</p>

Tabla 5-23. Configuración de SSH

Valor	Descripción
Activado	<p>Activa el SSH en el CMC.</p> <p>Valor predeterminado: seleccionado (activado)</p>
Nº máx. de sesiones	<p>El número máximo de sesiones simultáneas de SSH permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluyendo la suya).</p> <p>Rango configurable: 1 a 4</p> <p>Valor predeterminado: 4</p> <p>NOTA: Si cambia la propiedad Nº máx. de sesiones a un valor menor que el número de Sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.</p>
Tiempo de espera en inactividad	<p>Indica el número de segundos antes de que una sesión SSH sin actividad se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual.</p> <p>Rango de tiempo de espera: 0 o 60-10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0.</p> <p>Valor predeterminado: 1800 segundos</p>
Número de puerto	<p>El puerto utilizado por el CMC en espera de una conexión de servidor.</p> <p>Rango de configuración: de 10 a 65535</p> <p>Valor predeterminado: 22</p>

Tabla 5-24. Configuración de Telnet

Valor	Descripción
Activado	<p>Activa la interfaz de la consola Telnet del CMC.</p> <p>Valor predeterminado: sin seleccionar (desactivada)</p>
Nº máx. de sesiones	<p>Indica el número máximo de sesiones de Telnet simultáneas permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluyendo la suya).</p> <p>Rango permitido: 1 a 4</p> <p>Valor predeterminado: 4</p> <p>NOTA: Si cambia la propiedad Nº máx. de sesiones a un valor menor que el número de Sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.</p>
Tiempo de espera en inactividad	<p>Indica el número de segundos antes de que una sesión de Telnet se desconecte automáticamente. Un cambio en el valor del tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual.</p> <p>Rango de tiempo de espera: 0 o 60-10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0.</p> <p>Valor predeterminado: 1800 segundos</p>
Número de puerto	<p>Indica el puerto utilizado por el CMC que detecta una conexión con el servidor.</p> <p>Valor predeterminado: 23</p>

Tabla 5-25. Configuración de RACADM?remota

Valor	Descripción
Activado	Activa el acceso de la utilidad RACADM remoto al CMC. Valor predeterminado: seleccionado (activado)
Nº máx. de sesiones	Indica el número máximo de sesiones de RACADM simultáneas permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluyendo la suya). Rango permitido: 1 a 4 Valor predeterminado: 4 NOTA: Si cambia la propiedad Nº máx. de sesiones a un valor menor que el número de Sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.
Tiempo de espera en inactividad	Indica el número de segundos antes de que una sesión racadm inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera en inactividad tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Para desactivar la función Tiempo de espera en inactividad, introduzca 0. Rango de tiempo de espera: 0 o 10 hasta 1920 segundos. Para desactivar la función de tiempo de espera, introduzca 0. Valor predeterminado: 30 segundos

Configuración del presupuesto de alimentación

El CMC le permite presupuestar y administrar la alimentación para el chasis. El servicio de administración de alimentación optimiza el consumo de energía y reasigna la alimentación eléctrica a los distintos módulos en función de la demanda.

Para obtener instrucciones acerca de cómo configurar la energía mediante el CMC, consulte [Configuración y administración de energía](#).

Para obtener más información acerca del servicio de administración de energía del CMC, consulte [Administración de la alimentación](#).

Administración del firmware

En esta sección se describe cómo usar la interfaz web para actualizar el firmware. Los siguientes componentes se pueden actualizar mediante GUI o los comandos de RACADM:

- 1 CMC: principal y en espera.
- 1 iKVM
- 1 iDRAC (modo de bloqueo de inicio únicamente)
- 1 Servicios de infraestructura del módulo de E/S

Cuando se actualiza el firmware, se recomienda seguir un proceso que puede evitar una pérdida del servicio si la actualización falla. Consulte [Instalación o actualización del firmware de CMC](#) para obtener normas a seguir antes de utilizar las instrucciones de esta sección.

Cómo ver las versiones actuales del firmware

La página **Componentes que se pueden actualizar** muestra la versión actual del firmware de iKVM, el firmware del CMC principal, el firmware del CMC en espera (si corresponde), el firmware del iDRAC y el firmware del dispositivo de infraestructura del módulo de E/S. Al hacer clic en el nombre del dispositivo o en la versión del firmware, aparecerá la página **Actualización de dispositivos** para ese dispositivo particular.

La página **Actualización de dispositivos** aparece sólo una vez por dispositivo, excepto en el caso del CMC donde se muestra el CMC activo y en espera si ambos se pueden actualizar. Sólo el CMC activo y en espera se pueden actualizar al mismo tiempo en la misma acción desde la interfaz web; el resto de los dispositivos (módulos de E/S o servidores) deben actualizarse uno por vez. Para actualizar varios servidores y módulos de E/S, consulte [fwupdate](#) para obtener información acerca del comando `fwupdate`.

Si el chasis contiene un servidor cuyo iDRAC está en modo de recuperación o si el CMC detecta que un iDRAC tiene firmware dañado, el iDRAC también se enumera en la página **Componentes que se pueden actualizar**. Consulte [Recuperación del firmware del iDRAC por medio del CMC](#) para ver los pasos para recuperar el firmware del iDRAC mediante el CMC.

Para ver las versiones del firmware:

1. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
2. Haga clic en **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**.

Actualización del firmware

- 🔍 **NOTA:** Para actualizar el firmware del CMC, debe tener privilegios de **Administrador de configuración del chasis**.
- 🔍 **NOTA:** La actualización del firmware conserva la configuración actual del CMC y del iKVM.
- 🔍 **NOTA:** Si se utiliza una sesión de interfaz del usuario web para actualizar el firmware del componente del sistema, se debe configurar el valor del "Tiempo de espera en inactividad" para que se adecue al tiempo de transferencia de archivos. En algunos casos, es posible que el tiempo de transferencia de archivos de firmware sea de hasta 30 minutos. Para configurar el valor del "Tiempo de espera en inactividad", consulte [Configuración de servicios](#).
- 🔍 **NOTA:** El firmware del iDRAC se puede actualizar mediante la interfaz para el usuario basada en web del iDRAC o de RACADM remoto. Sin embargo, si la interfaz para el usuario del CMC detecta la presencia de un servidor pero no puede comunicarse con éste, indica una falla. En esos casos, la actualización del firmware del iDRAC estará disponible desde la página **Componentes que se pueden actualizar**. Para abrir la página **Componentes que se pueden actualizar**, seleccione **Chasis** en el árbol del sistema y luego haga clic en la ficha **Actualizar**.

La página **Componentes que se pueden actualizar** muestra la versión actual del firmware para cada componente enumerado y le permite actualizar el firmware a la revisión más reciente, cargando el archivo de imagen del firmware (paquete).

- 🔍 **NOTA:** Asegúrese de tener la versión más reciente del firmware. No puede descargar el archivo de imagen del firmware más reciente desde el sitio web de asistencia de Dell.

Actualización del firmware del CMC

- 🔍 **NOTA:** Durante las actualizaciones del firmware del CMC o del iDRAC en un servidor, algunas o todas las unidades de ventilador en el chasis girarán al 100%. Esto es normal.
- 🔍 **NOTA:** El CMC activo (principal) se restablecerá y no estará disponible temporalmente después de que el firmware se haya cargado satisfactoriamente. Si hay un CMC en espera, las funciones de actividad y espera se intercambiarán; el CMC en espera (secundario) será el CMC activo (principal). Si se aplica una actualización sólo al CMC activo (principal), después de que se haya completado el restablecimiento, el CMC principal no ejecutará la imagen actualizada, sólo el CMC en espera (secundario) tendrá dicha imagen.
- 🔍 **NOTA:** Para evitar que otros usuarios sean desconectados durante el restablecimiento, notifique a los usuarios autorizados que puedan tratar de iniciar sesión en el CMC y consulte la página **Sesiones** para ver si hay sesiones activas. Para abrir la página **Sesiones**, seleccione **Chasis** en el árbol, haga clic en la ficha **Red/seguridad** y después haga clic en la subficha **Sesiones**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.
- 🔍 **NOTA:** Al transferir archivos al CMC y desde el mismo, el icono de transferencia de archivos gira durante la transferencia. Si el icono no está animado, asegúrese de que el explorador esté configurado para permitir animaciones. Para obtener instrucciones, consulte [Habilitación de animaciones en Internet Explorer](#).
- 🔍 **NOTA:** Si experimenta problemas al descargar archivos desde el CMC usando Internet Explorer, active la opción **No guardar páginas cifradas en el disco**. Para obtener instrucciones, consulte [Descarga de archivos desde el CMC con Internet Explorer](#).

1. En la página **Componentes actualizables**, haga clic en el nombre de CMC. Aparece la página **Actualización de firmware**. El CMC activo, y si está presente, el CMC en espera, están enumerados y seleccionados. Ambos CMC pueden actualizarse al mismo tiempo.
2. En el campo **Imagen del firmware**, introduzca la ruta de acceso al archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para desplazarse a la ubicación del archivo.

- 🔍 **NOTA:** El nombre de la imagen del firmware del CMC predeterminado es **firmimg.cmc**. El firmware del CMC debe actualizarse primero, antes de actualizar el firmware del dispositivo de infraestructura del módulo de E/S.

3. Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.
4. Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar en gran medida según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Puntos adicionales para tener en cuenta:
 - 1 No utilice el botón **Actualizar** ni visite otra página durante la transferencia de archivos.
 - 1 Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**: esta opción sólo está disponible durante la transferencia de archivos.
 - 1 El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

- 🔍 **NOTA:** Es posible que la actualización lleve varios minutos para el CMC.

5. En un CMC en espera (secundario), el campo Estado de la actualización mostrará "Listo" cuando se complete la actualización. En un CMC activo (principal), durante las etapas finales del proceso de actualización del firmware, la sesión del explorador y la conexión con el CMC se perderá temporalmente ya que el CMC activo (principal) se retira de la línea. Debe iniciar sesión después de unos minutos, cuando el CMC activo (principal) se haya reiniciado.

Después de que se restablece el CMC, se actualiza el nuevo firmware y aparece en la página **Componentes que se pueden actualizar**.

- 🔍 **NOTA:** Después de actualizar el firmware, borre la caché del explorador de web. Consulte la ayuda en línea de su explorador de web para obtener instrucciones acerca de cómo borrar la caché del explorador.

Actualización del firmware de iKVM

 **NOTA:** Una vez que el firmware se ha cargado correctamente, se reinicia el iKVM y deja de estar disponible temporalmente.

1. Vuelva a iniciar sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**.
4. Haga clic en el nombre de iKVM. Aparece la página **Actualización de firmware**.
5. En el campo **Imagen del firmware**, introduzca la ruta de acceso al archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para desplazarse a la ubicación del archivo.

 **NOTA:** El nombre predeterminado de la imagen del firmware de iKVM es **kvm.bin**; sin embargo, el usuario lo puede cambiar.

6. Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.
7. Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar en gran medida según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Puntos adicionales para tener en cuenta:
 - 1 No utilice el botón **Actualizar** ni visite otra página durante la transferencia de archivos.
 - 1 Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**: esta opción sólo está disponible durante la transferencia de archivos.
 - 1 El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

 **NOTA:** La actualización puede llevar hasta un minuto para el iKVM.

Cuando se completa la actualización, iKVM se reinicia y el nuevo firmware se actualiza y aparece en la página **Componentes que se pueden actualizar**.

Actualización del firmware de los dispositivos de infraestructura del módulo de E/S

Al realizar esta actualización, se actualiza el firmware para un componente de la infraestructura del dispositivo del módulo de E/S.

1. Vuelva a iniciar sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**.
4. Haga clic en el nombre del dispositivo de la infraestructura del módulo de E/S. Aparece la página **Actualización de firmware**.
5. En el campo **Imagen del firmware**, introduzca la ruta de acceso al archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para desplazarse a la ubicación del archivo.

 **NOTA:** El campo **Imagen del firmware** no se muestra para un dispositivo de infraestructura del módulo de E/S de destino (IOMINKF) porque la imagen requerida reside en el CMC. El firmware del CMC debe actualizarse primero, antes de actualizar el firmware del dispositivo de infraestructura del módulo de E/S.

6. Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.
7. Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar en gran medida según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Puntos adicionales para tener en cuenta:
 - 1 No utilice el botón **Actualizar** ni visite otra página durante la transferencia de archivos.
 - 1 Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**: esta opción sólo está disponible durante la transferencia de archivos.
 - 1 El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

 **NOTA:** No aparecerá ningún cronómetro de transferencia cuando se actualiza el firmware de IOMINF. El proceso de actualización provocará una breve pérdida de la conectividad en el dispositivo del módulo de E/S porque el dispositivo se reiniciará cuando se complete la actualización.

Cuando se completa la actualización, el nuevo firmware se actualiza y aparece en la página **Componentes que se pueden actualizar**.

Actualización del firmware del iDRAC del servidor

 **NOTA:** El iDRAC (en un servidor) se reiniciará y no estará disponible temporalmente después de que se hayan cargado satisfactoriamente las actualizaciones del firmware.

1. Vuelva a iniciar sesión en la interfaz web del CMC.
2. Seleccione **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**.
4. Haga clic en el nombre del servidor. Aparece la página **Firmware Update (Actualización de firmware)**.
5. En el campo **Imagen del firmware**, introduzca la ruta de acceso al archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para desplazarse a la ubicación del archivo.
6. Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.
7. Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar en gran medida según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Puntos adicionales para tener en cuenta:
 - 1 No utilice el botón **Actualizar** ni visite otra página durante la transferencia de archivos.
 - 1 Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**: esta opción sólo está disponible durante la transferencia de archivos.
 - 1 El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

 **NOTA:** Es posible que la actualización lleve varios minutos para el CMC o el servidor.

Cuando finaliza la actualización, el servidor actualizado ya no aparecerá en la página **Componentes que se pueden actualizar**.

Recuperación del firmware del iDRAC por medio del CMC

El firmware del iDRAC se actualiza normalmente usando capacidades del iDRAC, como la interfaz web del iDRAC, la interfaz de línea de comando SM-CLP o los paquetes de actualización específicos del sistema operativo descargados desde support.dell.com. Consulte la *Guía del usuario del firmware del iDRAC* para ver instrucciones acerca de cómo actualizar el firmware del iDRAC.

Si el firmware del iDRAC se daña, como podría ocurrir si el progreso de actualización del firmware del iDRAC se interrumpe antes de terminar, usted puede usar la interfaz web del CMC para actualizar el firmware.

Si el CMC detecta el firmware del iDRAC dañado, el iDRAC aparecerá en la página **Componentes que se pueden actualizar**. Consulte [Cómo ver las versiones actuales del firmware](#) para obtener instrucciones acerca de cómo mostrar la página **Componentes que se pueden actualizar**.

 **NOTA:** Si la dirección MAC del iDRAC se ha perdido o dañado, se deberá establecer una dirección válida antes de poder recuperar el firmware del iDRAC por medio del CMC. Puede usar el comando **config params** de IPMI para establecer una dirección MAC. La dirección MAC es el quinto parámetro del comando. Debe establecerse una dirección de 6 bytes única en la red de administración. Consulte la documentación de la utilidad IPMI (por ejemplo, **ipmitool** o **ipmish**) para obtener ayuda para ejecutar el comando.

Siga estos pasos para actualizar el firmware del iDRAC.

1. Descargue el firmware del iDRAC más reciente en el equipo de administración de la dirección support.dell.com.
2. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
3. Haga clic en **Chasis** en el árbol del sistema.
4. Haga clic en la ficha **Actualizar**. Aparece la página **Componentes actualizables**. El servidor con el iDRAC que se puede recuperar se incluirá en la lista siempre se pueda recuperar a partir del CMC.
5. Haga clic en *server-n*, donde *n* es el número del servidor cuyo iDRAC desea recuperar.
6. Haga clic en **Examinar**, vaya a la imagen del firmware del iDRAC que descargó y haga clic en **Abrir**.

 **NOTA:** El nombre predeterminado de la imagen del firmware del iDRAC es **firmimg.imc**.

7. Haga clic en **Iniciar actualización del firmware**.

 **NOTA:** La actualización del firmware del iDRAC puede tardar hasta diez minutos. El icono de transferencia de archivos gira mientras la imagen del firmware se transfiere al CMC, pero no mientras el CMC transfiere la imagen al iDRAC.

Después de que el archivo de la imagen del firmware ha sido cargado al CMC, el iDRAC se actualizará a sí mismo con la imagen.

FlexAddress

Esta sección describe las pantallas de la interfaz web de la función FlexAddress. FlexAddress es una actualización opcional que permite que los módulos de los servidores reemplacen la identificación WWN/MAC asignada por la fábrica por una identificación WWN/MAC proporcionada por el chasis.

 **NOTA:** Debe adquirir e instalar la actualización FlexAddress para tener acceso a las pantallas de configuración. Si no se adquirió e instaló la actualización, aparecerá el siguiente texto en la interfaz web:

Optional feature not installed. See the *Dell Chassis Management Controller Users Guide* for information on the chassis-based WWN and MAC address administration feature.

To purchase this feature, please contact Dell at www.dell.com.

(Función opcional no instalada. Consulte la información de la *Guía del usuario de Dell Chassis Management Controller* para obtener información acerca de la función de administración de direcciones WWN y MAC basadas en el chasis.

Para adquirir esta función, póngase en contacto con Dell en www.dell.com.)

Cómo ver el estado de FlexAddress

Puede usar la interfaz web para ver información del estado de FlexAddress. Puede ver información del estado del chasis completo o de un servidor individual. La información que se muestra incluye:

- 1 Configuración de la estructura de red
- 1 FlexAddress activado/no activado
- 1 Número y nombre de la ranura
- 1 Direcciones asignadas por el chasis y por el servidor
- 1 Direcciones en uso

 **NOTA:** También puede ver el estado de FlexAddress a través de la interfaz de la línea de comandos. Para obtener más información acerca de los comandos, consulte [Uso de FlexAddress](#).

Cómo ver el estado de FlexAddress del chasis

La información del estado de FlexAddress se puede mostrar para todo el chasis. La información del estado incluye si la función está activada y una descripción general del estado de FlexAddress de cada cuchilla.

Siga los siguientes pasos para ver si FlexAddress está activado para el chasis:

1. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
2. Haga clic en **Chasis** en el árbol del sistema.
3. Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración general**. La entrada de FlexAddress tendrá un valor de **Activado** o **No activado**; el valor activado significa que la función está instalada en el chasis. El valor no activado significa que la función no está instalada ni en uso en el chasis.

Siga los siguientes pasos para mostrar un resumen general del estado de FlexAddress para cada módulo del servidor:

1. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
2. Haga clic en **Servidores** en el árbol del sistema. Haga clic en la ficha **Propiedades**, y luego en la subficha **WWN/MAC**.
3. Aparecerá la página **Resumen de FlexAddress**. Esta página le permite ver la configuración de WWN y las direcciones MAC para todas las ranuras del chasis.

La página de estado presenta la siguiente información:

Configuración de la estructura de red	Estructura de red A, Estructura de red B y Estructura de red C muestran los tipos de estructura de red de entrada/salida instalados.
Direcciones WWN/MAC	Muestra la configuración de FlexAddress para cada ranura del chasis. La información que se muestra incluye: <ul style="list-style-type: none">1 Número y ubicación de la ranura

	<ul style="list-style-type: none"> 1 Estado de FlexAddress activado/no activado 1 Tipo de estructura de red 1 Direcciones WWN/MAC en uso asignadas por el servidor y por el chasis <p>Una marca de selección verde indica el tipo de dirección activada, ya sea asignada por el servidor o por el chasis.</p>
--	--

4. Para obtener información adicional, haga clic en el vínculo **Ayuda** y revise [Uso de FlexAddress](#).

Cómo ver el estado de FlexAddress del servidor

La información del estado de FlexAddress también se puede mostrar para cada servidor individual. La información del nivel del servidor muestra una descripción general del estado de FlexAddress para esa cuchilla.

Siga los siguientes pasos para ver información del servidor de FlexAddress:

1. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
2. Expanda **Servidores** en el árbol del sistema. Todos los servidores (1-16) aparecen en la lista ampliada de **Servidores**.
3. Haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.
4. Haga clic en la ficha **Configuración**, y en la subficha **FlexAddress**. Aparecerá la página **Estado de FlexAddress**. Esta página le permite ver la configuración de WWN y las direcciones MAC para el servidor seleccionado.

La página de estado presenta la siguiente información:

FlexAddress activado	Muestra si la función FlexAddress está activada o no para la ranura particular.		
Estado actual	Muestra la configuración actual de FlexAddress: <ul style="list-style-type: none"> 1 Asignadas por el chasis: la dirección de ranura seleccionada es asignada por el chasis a través de FlexAddress. Las direcciones WWN/MAC basadas en la ranura son las mismas aún si se instala un nuevo servidor. 1 Asignadas por el servidor: el servidor usa la dirección asignada por el servidor o la dirección predeterminada integrada en el hardware del controlador. 		
Estado de la alimentación	Muestra el estado actual de la alimentación de los servidores; los valores son: Encendido , Encendiendo , Apagando , Apagado y N/A (si un servidor no está presente).		
Estado		En buen estado	Indica que FlexAddress está presente y proporciona estado al CMC. Si se presenta una falla en la comunicación entre el CMC y FlexAddress, el CMC no podrá obtener o mostrar los estados en los que se encuentra FlexAddress.
		Informativo	Muestra información acerca de FlexAddress cuando no se ha producido ningún cambio en el estado (En buen estado, Advertencia, Grave).
		Advertencia	Indica que sólo se han generado alertas de advertencia y que se debe realizar una acción correctiva dentro del tiempo establecido por el administrador . Si no se realizan

			acciones correctivas dentro del tiempo especificado por el administrador, se podrían producir fallas críticas o graves que podrían afectar la integridad del servidor.
	✘	Grave	Indica que se ha emitido al menos una alerta de falla. El estado grave representa una falla del sistema en el servidor y se debe realizar una acción correctiva inmediatamente.
		Sin valor	Cuando FlexAddress está ausente, no se proporcionará información de estado.
Firmware del iDRAC	Muestra la versión del iDRAC instalada actualmente en el servidor.		
Versión del BIOS	Muestra la versión actual del BIOS del módulo de servidores.		
Ranura	Número de ranura del servidor asociado con la ubicación de la estructura de red.		
Ubicación	Muestra la ubicación del módulo de E/S de entrada/salida en el chasis por número de grupo (A, B o C) y por número de ranura (1 o 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2.		
Estructura de red	Muestra el tipo de estructura de red.		
Asignadas por el servidor	Muestra las direcciones WWN/MAC asignadas por el servidor integradas en el hardware del controlador.		
Asignadas por el chasis	Muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para la ranura particular.		

5. Para obtener información adicional, haga clic en el vínculo **Ayuda** y revise [Uso de FlexAddress](#).

Configuración de FlexAddress

Si ha adquirido FlexAddress con el chasis, se instalará y activará al encender el sistema. Si ha adquirido FlexAddress más adelante, deberá instalar la tarjeta de función SD siguiendo las instrucciones del documento *Especificaciones técnicas de Chassis Management Controller (CMC) Secure Digital (SD) Card*. Visite la página support.dell.com para obtener este documento.

El servidor debe estar apagado antes de comenzar la configuración. Puede activar o desactivar FlexAddress por estructura de red. Además, puede activar/desactivar la función por ranura. Después de haber activado la función por estructura de red, puede seleccionar las ranuras que se activarán. Por ejemplo, si Estructura de red A está activada, todas las ranuras que estén activadas tendrán FlexAddress activado sólo en la Estructura de red A. El resto de las estructuras de red usarán la WWN/MAC asignada de fábrica en el servidor.

Las ranuras seleccionadas tendrán FlexAddress activado para todas las estructuras de red activadas. Por ejemplo, no es posible activar la Estructura de red A y B y tener la Ranura 1 con FlexAddress activado en la Estructura de red A pero no en la Estructura de red B.

 **NOTA:** También puede configurar FlexAddress a través de la interfaz de línea de comandos. Para obtener más información acerca de los comandos, consulte [Uso de FlexAddress](#).

Configuración FlexAddress para ranuras y estructuras de red a nivel del chasis

En el nivel del chasis, puede activar o desactivar la función FlexAddress para las estructuras de red y las ranuras. FlexAddress se activa por estructura de red y luego se seleccionarán las ranuras para su participación en la función. Tanto las estructuras de red como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Realice los siguientes pasos para activar o desactivar las estructuras de red y las ranuras para utilizar la función FlexAddress:

1. Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
2. Haga clic en **Servidores** en el árbol del sistema.
3. Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración general**. Haga clic en **Utilizar FlexAddress**. Aparecerá la página **Utilizar FlexAddress**.
4. La página **Seleccionar estructuras de red para WWN/MAC asignadas por el chasis** muestra una casilla de marcación para la **Estructura de red A**, **Estructura de red B** y **Estructura de red C**.

- Haga clic en la casilla de marcación de cada estructura de red para la que desea activar FlexAddress. Para desactivar una estructura de red, haga clic en la casilla de marcación para borrar la selección.

 **NOTA:** Si no se seleccionan las estructuras de red, FlexAddress no estará activado para las ranuras seleccionadas.

La página **Seleccionar ranuras para WWN/MAC asignadas por el chasis** muestra la casilla de marcación **Activada** para cada ranura en el chasis (1-16).

- Haga clic en la casilla de marcación **Activada** de cada ranura para la que desea activar FlexAddress. Si desea seleccionar todas las ranuras, utilice la casilla de marcación **Seleccionar/Deseleccionar todo**. Para desactivar una ranura, haga clic en la casilla de marcación **Activada** para borrar la selección.

 **NOTA:** Si la cuchilla está presente en la ranura, debe ser apagada antes de que se active la función FlexAddress en esa ranura.

 **NOTA:** Si no se seleccionan las ranuras, FlexAddress no estará activado para las estructuras de red seleccionadas.

- Haga clic en **Aplicar** para guardar los cambios.

- Para obtener información adicional, haga clic en el vínculo **Ayuda** y revise [Uso de FlexAddress](#).

Configuración de FlexAddress de ranuras a nivel del servidor

En el nivel del servidor, puede activar o desactivar la función FlexAddress para ranuras individuales.

Siga los siguientes pasos para activar o desactivar una ranura individual para utilizar la función FlexAddress:

- Inicie sesión en la interfaz web (consulte [Acceso a la interfaz web del CMC](#)).
- Expanda **Servidores** en el árbol del sistema. Todos los servidores (1-16) aparecen en la lista ampliada de **Servidores**.
- Haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.
- Haga clic en la ficha **Configuración**, y en la subficha **FlexAddress**. Aparecerá la página **Estado de FlexAddress**.
- Utilice el menú desplegable de **FlexAddress activado** para realizar la selección; seleccione **Sí** para activar FlexAddress o seleccione **No** para desactivar FlexAddress.
- Haga clic en **Aplicar** para guardar los cambios. Para obtener información adicional, haga clic en el vínculo **Ayuda** y revise [Uso de FlexAddress](#).

Preguntas más frecuentes

La [tabla 5-26](#) contiene las preguntas y respuestas frecuentes.

Tabla 5-26. Administración y recuperación de un sistema remoto: Preguntas frecuentes

Pregunta	Respuesta
Al acceder a la interfaz web del CMC, recibo una advertencia de seguridad informando que el nombre del host del certificado SSL no coincide con el nombre del host del CMC.	<p>El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Cuando se usa este certificado, el explorador de web muestra una advertencia de seguridad porque el certificado predeterminado se emite para el Certificado predeterminado del CMC, que no coincide con el nombre del host del CMC (por ejemplo, la dirección IP).</p> <p>Para resolver este problema de seguridad, cargue un certificado de servidor del CMC que haya sido emitido para la dirección IP del CMC. Al generar la solicitud de firma de certificado (CSR) que se usará para emitir el certificado, asegúrese de que el nombre común (CN) de la CSR tenga la misma dirección IP que el CMC (por ejemplo, 192.168.0.120) o el mismo nombre DNS registrado que el CMC.</p> <p>Para asegurarse de que la CSR coincida con el nombre DNS registrado del CMC:</p> <ol style="list-style-type: none"> En el árbol Sistema, haga clic en Chasis. Haga clic en la ficha Red/Seguridad y luego haga clic en Configuración. Aparecerá la página Configuración de la red. Seleccione la casilla de marcación Registrar el CMC en DNS. Introduzca el nombre del CMC en el campo Nombre del CMC en DNS. Haga clic en Aplicar cambios.
	Para obtener más información acerca de cómo producir CSR y cómo emitir certificados, consulte Protección de las comunicaciones del CMC con certificados SSL y digitales .

<p>¿Por qué no están disponibles los servicios de RACADM remoto y de web después de un cambio de propiedad?</p>	<p>Es posible que los servicios de RACADM remoto y de la interfaz web tarden un minuto para estar disponibles después de que el servidor de web del CMC se restablezca.</p> <p>El servidor de web del CMC se restablece después de los siguientes acontecimientos:</p> <ul 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 usuario de web del CMC 1 Cuando la propiedad <code>cfgRacTuneHttpsPort</code> cambia (incluso cuando un comando <code>config -f <archivo_de_config></code> la cambia) 1 Cuando se utiliza <code>racresetcfg</code> 1 Cuando el CMC se restablece 1 Cuando se carga un nuevo certificado de servidor SSL
<p>¿Por qué mi servidor DNS no registra mi CMC?</p>	<p>Algunos de los servidores DNS sólo registran nombres de 31 caracteres o menos.</p>
<p>Al acceder a la interfaz web del CMC, recibo una advertencia de seguridad informando que el certificado SSL fue emitido por una autoridad de certificados que no es confiable.</p>	<p>El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Este certificado <i>no</i> es emitido por una autoridad de certificados confiable. Para resolver este problema de seguridad, cargue un certificado de servidor del CMC que haya sido emitido por una autoridad de certificados confiable (por ejemplo, Thawte o Verisign). Para obtener más información acerca de cómo emitir certificados, consulte Protección de las comunicaciones del CMC con certificados SSL y digitales.</p>
<p>El mensaje siguiente se muestra por motivos desconocidos:</p> <p>Acceso remoto: error 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, usted tiene el nombre de comunidad Get = public y el nombre de comunidad Get = private. De manera predeterminada, el nombre de comunidad para el agente CMC es "public" (público). Cuando IT Assistant envía una solicitud de comunidad Set, el agente CMC genera el error de autenticación SNMP porque sólo acepta solicitudes de comunidad = public (público).</p> <p>Puede cambiar el nombre de comunidad del CMC por medio de RACADM.</p> <p>Para ver el nombre de comunidad del CMC, use el comando siguiente:</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>Para establecer el nombre de comunidad del CMC, 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 CMC sólo permite un nombre de comunidad, debe introducir el mismo nombre de comunidad Get y Set para la configuración de descubrimiento de IT Assistant.</p>

Solución de problemas del CMC

La interfaz web del CMC proporciona herramientas para identificar, diagnosticar y corregir problemas del chasis. Para obtener más información acerca de la solución de problemas, consulte [Solución de problemas y recuperación](#).

[Regresar a la página de contenido](#)